Defence Research and Development Canada
Recherche et développement pour la défense Canada

DEFENCE R&D DÉFENSE

Comparison of Two Hierarchical Routing Protocols for Heterogeneous MANET

Maoyu Wang, Ying Ge and Louise Lamont

The work described in this document was sponsored by the Department of National Defence under Work Unit 15BR.

Defence R&D Canada – Ottawa
TECHNICAL MEMORANDUM
DRDC Ottawa TM 2007-201
October 2007

Canada

Comparison of Two Hierarchical Routing Protocols for Heterogeneous MANET

Maoyu Wang, Ying Ge and Louise Lamont
Communications Research Centre Canada

The work described in this document was sponsored by the Department of National Defence under Work Unit 15BR

Defence R&D Canada – Ottawa

Technical Memorandum

DRDC Ottawa TM 2007-201

October 2007

Abstract

In this report, a study on hierarchical routing protocols for heterogeneous mobile Ad Hoc wireless networks is presented. The main thrust of the investigation is to identify a potential hierarchical routing scheme that is best suited for a heterogeneous tactical Mobile Ad Hoc Network (MANET). Such networks consist of mobile nodes that are characterized by different communications capabilities, such as multiple radio interfaces. The report highlights the benefits and issues of the different routing protocols, namely the H-OLSR and H-LANMAR, as they pertain to a military tactical scenario. We first discuss the context for the use of a hierarchical routing strategy by describing a typical military scenario where a number of platforms are used each supporting link types of varying capabilities. We then discuss the rational for selecting a proactive hierarchical routing scheme for typical tactical MANETs. We discuss in detail the routing algorithms of the two protocols under investigation. Finally we conduct an experimental comparison study between the two routing protocols.

Our experiments reveal that H-OLSR outperforms H-LANMAR for most of the group mobility scenarios that can potentially be used in the operation of a tactical MANET.

Résumé

Dans ce rapport, on présente une étude portant sur les protocoles de routage hiérarchisé pour les réseaux ad hoc mobiles (MANET) hétérogènes. Il s'agit principalement de trouver le mode possible de routage hiérarchisé qui conviendrait le mieux à de tels MANET hétérogènes. Ces réseaux comprennent des nœuds mobiles aux capacités différentes de communication (interfaces radio multiples, etc.). Le document met en évidence les avantages et les difficultés que présentent les différents protocoles de routage, c'est-à-dire H-OLSR et H-LANMAR, en ce qui concerne un scénario militaire du domaine tactique. On examine d'abord le contexte de l'application d'une stratégie de routage hiérarchisé en décrivant un scénario militaire type où diverses plateformes servent au soutien de diverses capacités de liaison. Il est ensuite question de la justification du choix d'un mode proactif de routage hiérarchisé pour les MANET classiques du domaine tactique. On décrit en détail les algorithmes de routage relevant des deux protocoles considérés. Il y a enfin étude comparative par expérience des deux protocoles de routage. Les expériences en question révèlent que le protocole H-OLSR est d'un rendement supérieur au protocole H-LANMAR pour la plupart des scénarios de mobilité de groupe qui portent sur les déploiements types d'un MANET du domaine tactique.

This page intentionally left blank.

Executive Summary

Comparison of Two Hierarchical Routing Protocols for Heterogeneous MANET
Maoyu Wang, Ying Ge, Louise Lamont; DRDC Ottawa TM 2007-201; Defence R&D Canada – Ottawa; October 2007.

Wireless mobile ad hoc networking is increasingly becoming a key component for many civilian and military applications. Mobile Ad hoc Networks (MANETs) are autonomous systems of mobile nodes interconnected by wireless links. Intermediate mobile nodes in the MANET act as mobile routers to support connectivity to other mobile nodes that are out of each other's range. The mobile routers are free to move randomly and organize themselves arbitrarily. A unit (node) can join or leave a MANET and groups of nodes can merge or separate causing the network topology to change constantly. Nodes adapt to the rapid topology changes by recalculating new routes in order to keep connectivity. Different ad hoc routing schemes have been proposed to support communications in a MANET. In general, routing protocols for MANETs can be classified, in terms of the triggering mechanism used to broadcast control messages, as proactive, reactive or hybrid. Most of the routing protocols proposed for MANETs make the assumption that the ad hoc network is homogenous. That is, all the mobile nodes have the same capabilities in terms of processing capacity and in terms of the number of radio and/or networking interfaces. On the other hand, many contemporary ad hoc wireless networks are heterogeneous in nature, being comprised of mobile devices equipped with interfaces having distinct communications capabilities with respect to data rate, radio range, frequency band, battery life, etc.

In this report we investigate two different hierarchical routing schemes to facilitate the use and the design of a mobile ad hoc network for tactical operations. Our goal is to set a direction for the selection of a routing scheme for a typical tactical MANET. We start by giving a context for the use of a hierarchical routing strategy by describing a typical military scenario where a number of platforms are used each supporting link types of varying capabilities. We then discuss the rational for selecting a proactive hierarchical routing scheme for typical tactical MANETs. Due to the active research in this area, many routing protocols have been developed for applications that support a flat MANET architecture. These protocols where not optimally designed for a tactical MANET topology where nodes are characterized by different communications capabilities, such as multiple radio interfaces. We therefore present in detail two different routing schemes that are well suited for a tactical heterogeneous MANET topology. We use group mobility scenarios that characterize typical network operation of a tactical MANET. The goal is to show the strengths and weaknesses of the protocols under study in order to select the best resulting one.

H-LANMAR and H-OLSR are the two hierarchical routing schemes investigated in this report. H-LANMAR and H-OLSR support heterogeneous networks in different ways. H-LANMAR employs one type of routing scheme for a destination located inside a logical group and another scheme for a destination outside a logical group. H-OLSR introduces the concept of clusters and cluster heads to adapt to the heterogeneous network structure and uses the same routing scheme regardless of the destination node's

location. Our study shows that when nodes move strictly within their group area and the network traffic load is not too heavy, H-OLSR and H-LANMAR perform the same. For all other cases, H-OLSR outperforms H-LANMAR in terms of the packet delivery ratio and the end-to-end delay to varying degrees depending on the scenario at hand. Our recommendation is to select H-OLSR as a candidate hierarchical proactive routing protocol for military tactical scenarios.

Sommaire

Comparaison de deux modes de routage hiérarchisé pour une topologie de MANET hétérogène

Maoyu Wang, Ying Ge, Louise Lamont; DRDC Ottawa TM 2007-201; R et D pour la défense Canada – Ottawa; Octobre 2007.

Les réseaux ad hoc mobiles (MANET) en sans-fil tiennent une place de plus en plus essentielle dans un grand nombre d'applications civiles et militaires. Les MANET sont des systèmes autonomes de nœuds mobiles (dispositifs utilisateurs portatifs) en interconnexion sans-fil. Dans un MANET, les nœuds mobiles intermédiaires sont des routeurs mobiles qui assurent la connectivité avec d'autres nœuds mobiles hors de portée des premiers. Ces routeurs sont libres de se déplacer au hasard et de s'organiser arbitrairement. Une unité ou nœud peut gagner ou quitter un MANET et des groupes de nœuds peuvent être en jonction ou en disjonction, d'où une constante variation de la topologie du réseau. Les nœuds s'adaptent à ces variations rapides en calculant de nouvelles routes de maintien de la connectivité. On a proposé différents modes de routage ad hoc pour le soutien des communications dans un MANET. En général, les protocoles de routage MANET peuvent se caractériser selon le caractère proactif, réactif ou hybride du mécanisme déclencheur servant à la diffusion des messages de contrôle. Dans la plupart des protocoles de routage proposés pour les MANET, on suppose que ces réseaux sont homogènes, c'est-à-dire que tous les nœuds mobiles sont d'une même capacité pour le potentiel de traitement et le nombre d'interfaces radio et/ou réseau. Il reste que beaucoup de réseaux ad hoc contemporains en sans-fil sont hétérogènes, comprenant des dispositifs mobiles munis d'interfaces dont la capacité de communication diffère selon le débit de données, le radioalignement, la bande de fréquences, la durée utile des piles, etc.

Dans ce rapport, nous regardons deux modes de routage hiérarchisé qui facilitent la conception et l'exploitation d'un réseau ad hoc mobile pour des forces de coalition, le but étant d'orienter le choix d'un plan de routage pour un MANET type du domaine tactique. Nous établissons d'abord le contexte du recours à une stratégie de routage hiérarchisé en décrivant un scénario militaire type où diverses plateformes servent au soutien de diverses capacités de liaison. Nous examinons ensuite la justification du choix d'un mode proactif de routage hiérarchisé pour les MANET types du domaine tactique. Comme les chercheurs sont actifs dans ce domaine, on a mis au point un grand nombre de protocoles de routage pour des applications de soutien d'une architecture MANET unie. Ces protocoles n'ont rien d'optimal pour une topologie de MANET tactique où les nœuds diffèrent selon leur capacité de communication (interfaces radio multiples, etc.). Nous détaillons donc deux modes de routage qui conviennent bien à une topologie de MANET hétérogène du domaine tactique. Nous recourons à des scénarios de mobilité de groupe qui caractérisent l'exploitation normale d'un MANET tactique. Le but est de décrire les forces et les faiblesses des protocoles considérés pour que le meilleur puisse être choisi.

Dans ce rapport, les deux modes de routage hiérarchisé qui sont examinés sont les protocoles H-LANMAR et H-OLSR applicables à un soutien bien précis de réseaux hétérogènes. Dans le premier cas, on emploie un mode de routage d'un certain type pour une destination intragroupe logique et d'un autre type pour une destination extragroupe.

Dans le second cas, on adopte le concept de groupage et de tête de groupe pour s'adapter à la structure hétérogène du réseau, et on emploie le même mode de routage, quelle que soit la position du nœud de destination. Notre étude montre que, si les nœuds se déplacent strictement à l'intérieur de leur secteur de groupage et que le trafic réseau n'est pas trop lourd, H-OLSR et H-LANMAR ont le même rendement. Dans tous les autres cas, le premier de ces protocoles est d'un rendement supérieur au second pour ce qui est du débit en paquets et de la latence de bout en bout, et ce, à des degrés divers selon le scénario considéré. Notre recommandation est de choisir H-OLSR comme protocole proactif de routage hiérarchisé pour les scénarios militaires du domaine tactique.

Table of Contents

List of Figures

This page intentionally left blank.

1. Introduction

A Mobile Ad Hoc Network (MANET) is a dynamic multi-hop wireless network that consists of a group of mobile nodes on a shared wireless channel. Such a network may be self-contained, or it may be subsumed under a larger network. However, because member nodes are capable of random (individual) movement, network topology can change rapidly and unpredictably. Compared to a fixed-network architecture, an ad hoc network promises great features, such as the ability to instantly deploy mobile nodes, and the mobile nodes' ability of reconfiguring and of preserving connectivity during topology changes. These features of ad hoc networks offer several interesting areas of study.

Most of the routing protocols proposed for MANETs make the assumption that the ad hoc network is homogenous. That is, all the mobile nodes have the same capabilities in terms of processing capacity and in terms of the number of radio and/or networking interfaces. On the other hand, many contemporary ad hoc wireless networks are heterogeneous in nature, being comprised of mobile devices equipped with interfaces that have distinct communications capabilities with respect to data rate, radio range, frequency band, battery capacity, etc. In military networks for instance, soldiers, tanks and headquarters might each be given wireless communication equipment that is appropriate to their communication needs. Soldiers are usually equipped with wireless communication devices characterized by limited resources. Those devices can only handle limited transmission range and have restricted communications bandwidth[1]. Vehicles, on the other hand, are outfitted with more powerful equipments providing extended communication coverage with higher communication bandwidth[1] capability. Moreover, UAVs are equipped with additional interfaces providing direct point-to-point wireless communications with other UAV's, using their own carrier frequencies.

Scalability is one of the most important factors governing the efficiencies of heterogeneous wireless networks. Scalability may be defined as the ability of a network to adjust or maintain its performance when its size increases. That also includes the increase in traffic load that is handled. Yet under the existing "flat" routing protocol, the performance of an ad hoc network tends to degrade as the number of mobile nodes increases, because a flat routing protocol cannot differentiate the communication capacities of its member nodes, and does not scale well for typical heterogeneous networks of the type just described. When a flat routing protocol is used, the resulting control overhead increases, depending on the number of interfaces possessed by each node. More importantly, the high-capacity links are not efficiently exploited under such a routing strategy. For example, two nodes are connected by two interfaces with different link capacities. A flat routing protocol, without differentiating

[1] The term bandwidth used in this context means the raw data rate.

link capacities, will randomly select one interface for transmission instead of picking the high capacity one.

In this report, we discuss the suitability of a hierarchical structure MANET routing scheme when a tactical MANET is composed of different link capacities. We describe the functionality of two proactive hierarchical routing protocols that can be used in a typical tactical MANET. We present the results of the study that compares the routing protocols for different mobility patterns and offer some recommendations and suggestions.

2. Military Tactical Scenario

2.1 Scenario

The purpose of the scenario [1] introduced in this chapter is to provide an operational framework to define the scale of the network involved and facilitate the design of a mobile ad hoc network for coalition forces. The scenario forms an illustrative example for choosing standards for the communication links and helps to provide a context for the security analysis of the standards.

Military scenarios may be classified by their geographical coverage and the size of the mission. They may be grouped into strategic, operational, and tactical scenarios. In this project, a tactical scenario is used for designing a mobile ad hoc network. Its limited size makes it manageable, and its structure provides a good example for the application of a MANET.

The scenario is a tactical peacekeeping mission involving a coalition force. The tactical scenario consists of two phases. Phase one is the intelligence, surveillance, and reconnaissance (ISR) mission to identify and inspect suspected biochemical-manufacturing facilities. Phase two is establishing and maintaining the security of the suspect area. The scenario also incorporates the post-ISR ad hoc communication that is required to maintain the security of the manufacturing area. This is depicted in ***Figure 2.1.1***.

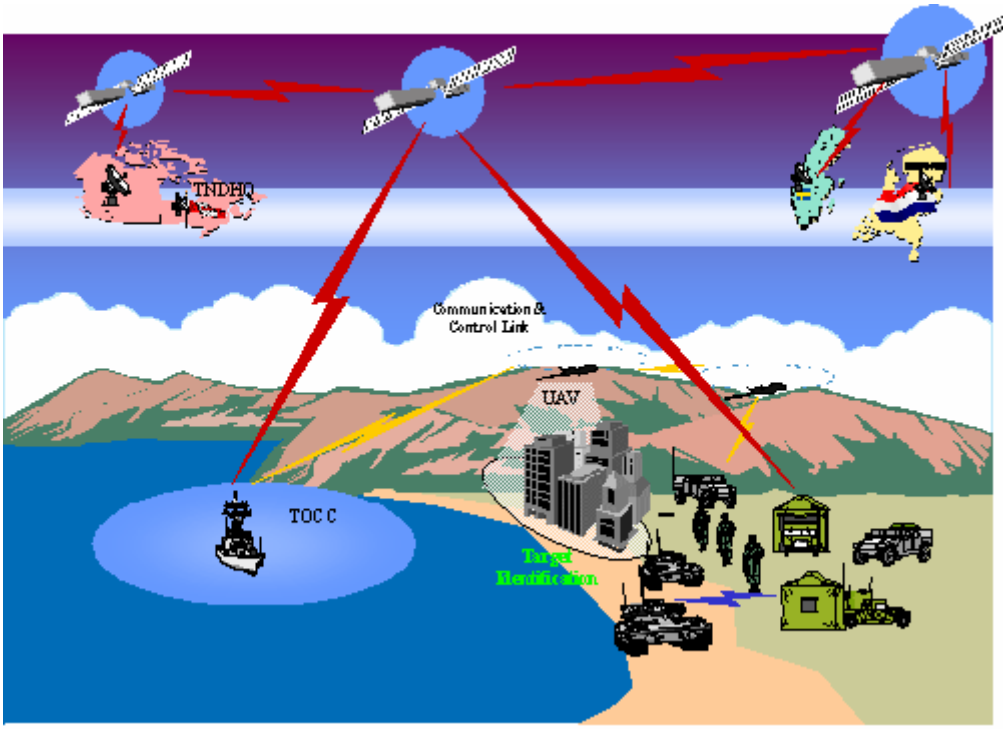

Figure 2.1.1 Tactical Theatre

The participating forces and platforms are:

- Transnational Operational Command Centre (TOCC) aboard a ship with links back to national strategic command centers and to the Transnational Defence Headquarters (TNDHQ);
- Unmanned aerial vehicles (UAVs) equipped to conduct wide area surveillance:
  - low altitude and short endurance for reconnaissance
  - high altitude and long endurance as a communications access point
- Armoured Personnel Vehicles (APVs);
- Foot soldiers for reconnaissance and control of suspected sites.

The required information exchanges via mobile ad hoc networks are soldier to soldier, soldier to APV, APV to TOCC, UAV to TOCC, UAV to APV, and others. Examples of applications that require security are collaborative planning, situational awareness, messaging, data transmission, UAV control, etc.

In phase one (ISR) an army controlled UAV equipped with an infrared camera, gas sensors, and a wireless communication link is remotely operated and controlled near the suspected factory. The information is relayed to the TOCC over a secure link to the ship, where an executive officer verifies the target, and where the information is then processed and sent to the TNDHQ via satellite.

In phase two (securing the theatre) the company of tanks and APVs moves in and secures the area after target identification has been completed. At least one army or navy controlled UAV continues to perform "lookout tasks" and provides the communications relay between the theatre area and the ship. The tanks and APVs use peer-to-peer communication. One tank secures an area between two mountains and acts as a relay between the theatre and the troops on the other side of the mountain. Some tanks or APVs and ground troops may have dedicated satellite links for connectivity with their national defence headquarters. The ground troops keep the public away from the factory and are equipped with notebook-like personal information systems. If the soldiers are within range of a tank, the tank acts as the relay point within the hierarchy of the architecture (which saves battery power and allows for the least expensive route possible), otherwise the soldier relays through the UAV.

2.2 Link Types

Nine different link types, indicated by numbers 1 to 9 as shown in ***Figure 2.2.1***, are identified for the scenario. Table 1.1 describes each of the links.

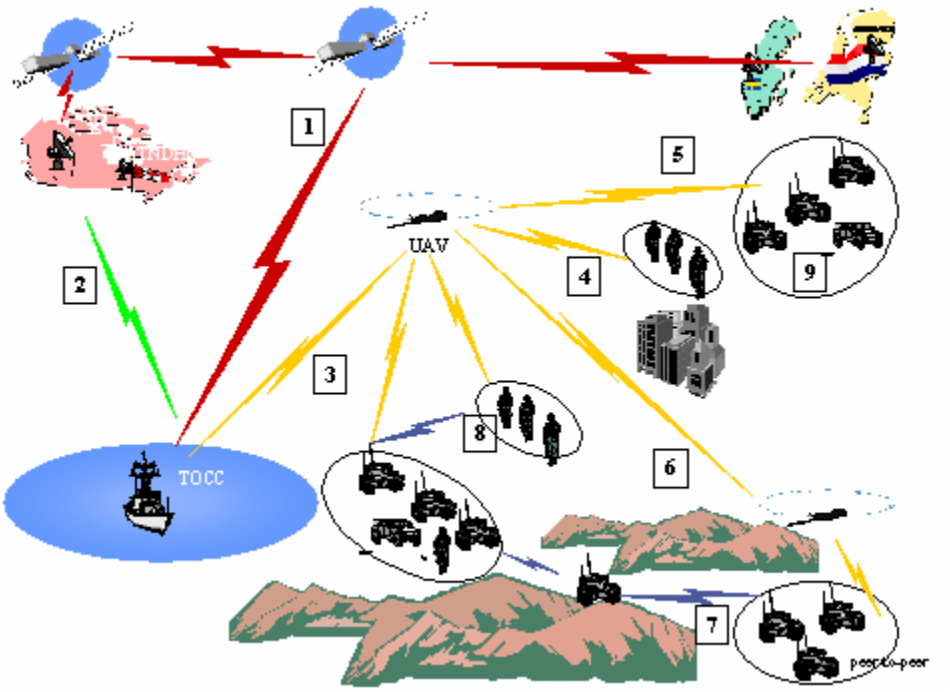

Figure 2.2.1 Link Types in the Scenario

1	Communication link between TOCC and TNDHQ using SATCOM
2	Backup communication link between TOCC and TNDHQ using HF radio
3	Communication link between TOCC and the UAV for controlling the UAV and data
4	UAV base station/access point for communication support, personnel mounted
5	UAV base station/access point for communication support, vehicle mounted
6	UAV to UAV relay link for data only
7	Peer-to-peer multi-hop relay link
8	Pedestrian ad hoc networking and pedestrian-to-vehicle relay
9	Vehicular ad hoc networking

Table 2.2.1 Link type definitions

2.3 Connectivity in the Tactical Scenario

There are two fundamental technology areas that can be used to provide connectivity between the various participating forces and platforms described in the previous scenario: *dynamic wireless routing* technology, and *edge mobility* technology.

Dynamic wireless routing technology is used in a MANET where a group of mobile, wireless nodes act as routers and forward traffic for other nodes in the network. The goal is to maintain connectivity between the MANET nodes by quickly finding efficient routes through the network, and maintaining these routes under dynamic conditions. Dynamic wireless routing is of most value when the intention is to form topologically unplanned networks. This can be as a result of the method of network deployment or, more usually, as a result of (ongoing) mobility within the network.

At the Front Line of Own Troops (FLOT), sections of dismounted soldiers may be tasked with an objective requiring them to move around one another as they tackle their objective. It is crucial that the soldiers are free to manoeuvre as the operational situation (rather than the communications constraints) dictates. Dynamic wireless routing treats each member of the section as a relay in order to pass information (voice or data) between members that are not within direct wireless range of each other. This property provides a transparent range extension in order to support extended manoeuvre.

Behind FLOT, tactical backbone networks are required to link together Headquarters in order to update one another with operational developments and commands from higher authorities. These tactical HQs can be moving periodically to avoid detection, but the location of their destination may only recently have been decided, thus forcing the formation of unplanned network topologies. Dynamic wireless routing copes gracefully with these situations by automatically forming opportunistic links with neighbours whenever they are within range of one another. Dynamic, wireless routing can also be used to rapidly establish wireless LAN communications around a deploying HQ without the need for an RF survey of the area; additional relay nodes are deployed until the desired level of connectivity is established.

Edge mobility focuses on mobile users, systems, or even entire mobile networks that are capable of macro-mobility, moving across routing borders and within a larger wide area network (WAN). The main edge mobility technologies are Mobile IP, designed to support individual roaming mobile hosts, and network mobility (NEMO) concepts, designed to support roaming aggregate networks. These technologies are often useful if the roaming node or network need to maintain existing connections while undergoing roaming conditions. Although the NEMO technology is not the focus of this report, the concepts and applicability to the military tactical scenario are worthwhile discussing for further research considerations and are presented in Appendix A. This report focuses on hierarchical routing strategies that efficiently exploit different link capacities has suggested in the tactical scenario presented earlier.

3. Proactive Hierarchical Routing Schemes For Military Tactical Network

When designing a routing scheme for a large scale MANET, an important feature to consider is whether or not the network is homogeneous or heterogeneous. Most MANET routing protocols are designed for homogeneous networks, where all nodes have the same processing and communication capability. However in most military tactical scenarios, MANETs are heterogeneous in nature and are comprised of mobile devices equipped with interfaces having distinct communications capabilities.

Current MANET protocols that are designed for homogeneous ad hoc networks can be largely divided into proactive and reactive protocols. In a proactive protocol (e.g. Optimized Link State Routing protocol, OLSR), each router node in the network constantly maintains a route to every other node in the MANET network. On the other hand, reactive protocols (e.g. Ad-Hoc On-Demand Distance Vector routing protocol, AODV) search for and maintain routes to destination nodes upon demand from user traffic. Each of these methods has different performance characteristics, dependent upon the scenario of use. For example, proactive protocols may produce more network overhead under sparse user traffic loads than reactive protocols, due to the control messages required to maintain routes when the routes may not be needed. Of course, depending on the number of sender/receiver pairs and the frequency of communication, this overhead may not be significant when compared to a reactive protocol, particularly in a traffic scenario where many nodes are receiving data as may often be the case in tactical networks. Reactive protocols, on the other hand, tend to produce larger initial connection delay than proactive protocols, due to the time it takes to find a route when data needs to be sent. Protocols such as OLSR and AODV support nodes having multiple interfaces. However they employ a "flat" mechanism, whereby a node sends its control messages through all its interfaces without regard to the link capacities of the other nodes. The resulting control overhead increases depending on the number of network interfaces possessed by the nodes.

There are also other protocols that have both proactive and reactive aspects to provide a more balanced design. Zone Routing Protocol (ZRP) [2] [3] falls into this category and is referred to as a hybrid protocol. ZRP provides a routing framework where each node maintains local routes within its local neighborhoods (routing zones) in a pro-active manner, while inter-zone communication is performed in a reactive manner. ZRP does not provide a single protocol, but outlines a routing framework for the inclusion and extensions of exiting ad hoc routing protocols. Access to a ZRP routing zones is provided not through a single cluster head or landmark but through the best peripheral nodes that define the extent of the zone. Communication beyond a

routing zone is passed across overlapping routing zones in a peer-to-peer manner, rather to a higher tier with broader coverage. For this reason ZRP is categorized as a flat routing protocol rather than a hierarchical one. ZRP can be used in a large homogeneous network but its flat framework is not suited for heterogeneous features.

In order to address the complex problem of routing in heterogeneous ad hoc networks, the network can be broken down into a hierarchy of smaller networks, where each level is responsible for its own routing. In hierarchical routing, routers are classified in groups known as regions. Each router has the complete information about the routers in its own region, and only has a piece of general information about routers in other regions. Additionally, in a hierarchical routing system, some routers act as a routing backbone. Packets from non-backbone routers travel to the backbone routers, where they are sent through the backbone until they reach the general area of the destination. At this point, they travel from the last backbone router through one or more non-backbone routers to the final destination.

Most existing hierarchical ad hoc routing protocols are derived from a "flat" ad routing protocol. For instance, H-AODV [8] and H-DSR [11] are examples of protocols that are based on the popular reactive routing protocols AODV [9] and DSR [12] while H-OLSR and H-LANMAR are derived from the proactive OLSR [13] and LANMAR [4].

In H-AODV, both backbone nodes and ordinary nodes run the same AODV routing protocol, where a route is discovered on the fly whenever there is a connection request. However, the backbone nodes broadcast RREQ [9] packets throughout the backbone network in addition. The key point of H-AODV is that the route discovery procedure can take advantage of the physical hierarchy. Thus, the backbone links are usually utilized to route packets to remote destinations. H-DSR was introduced in the Safari [11] project. A mobile ad hoc network self-organizes itself as cells. Each cell has a self-elected drum. All the drums form a new level in the hierarchy. For example if a network comprises of two levels, every node will belong to a specific cell at the first level. Several cells in the first layer form a larger cell and this will be referred to as the second level cell. A drum will be elected also at the second level cell. A node always associates with its first level drum and its higher-level drums. A packet travelling to a destination node will be directed to the destination node's highest-level drum first. In this case, it is directed to the destination node's second-level drum. Along the path, it may be directed to destination node's first-level drum. Following the path to its first-level drum, a packet enters the destination's first-level cell. The packet is delivered by DSR [12] to the final sink within the first-level cell. The path from drum to drum is created in a proactive fashion. Routing inside a cell is built using the DSR protocol. In flat networks, both H-AODV and H-DSR provide better scalability as the network size grows, a common feature of reactive protocols. However, reactive routing protocols as we have mentioned earlier suffer from the extreme connection delay for the first packet to be delivered. The long connection

delay is not acceptable for military applications, especially for time-critical military missions. Thus, we focus on the proactive routing protocols, as proactive routing ensures a minimum connection delay, which is essential in a military scenario.

H-OLSR and H-LANMAR are two proactive hierarchical routing protocols that can accommodate the military tactical scenario described earlier. Both H-OLSR and H-LANMAR utilize a hierarchical structure to reduce the routing overhead and to improve the protocol scalability for large-scale heterogeneous networks. However, the two proactive hierarchical routing protocols approach the hierarchical structure and improve the scalability in different manners, as we will discuss in the next sections of this report.

3.1 H-LANMAR

3.1.1 Introduction to LANMAR

Landmark Ad Hoc Routing (LANMAR) [4][5] is a routing protocol that exploits the landmark concept to handle group mobility in a scalable and mobile ad hoc network. The LANMAR routing protocol assumes that a large scale MANET consists of several logical groups. The assumption in LANMAR is that nodes having common interests are likely to move together and form a group. A landmark serves as the representative in each logical group. Nodes within a logical group know the exact routes to other members in the same logical group by using an in-scoped routing mechanism. A packet destined to nodes within the same group is sent to the destination directly (i.e. using intermediate relay nodes within the logical group). When a packet is destined to a destination that is not within the same group as the source node, the packet is initially directed towards the landmark instead of the destination itself; as it gets closer to destination it eventually switches to the accurate route provided by the in-scoped routing protocol.

Routing Table of Node C.1

Dest.	Next hop
C.2	C.2
C.3	C.3
C.4	C.2
C.5	C.3
C.6	C.2
Landmark A	A.7
Landmark B	C.2
Landmark D	D.3
Landmark E	C.3

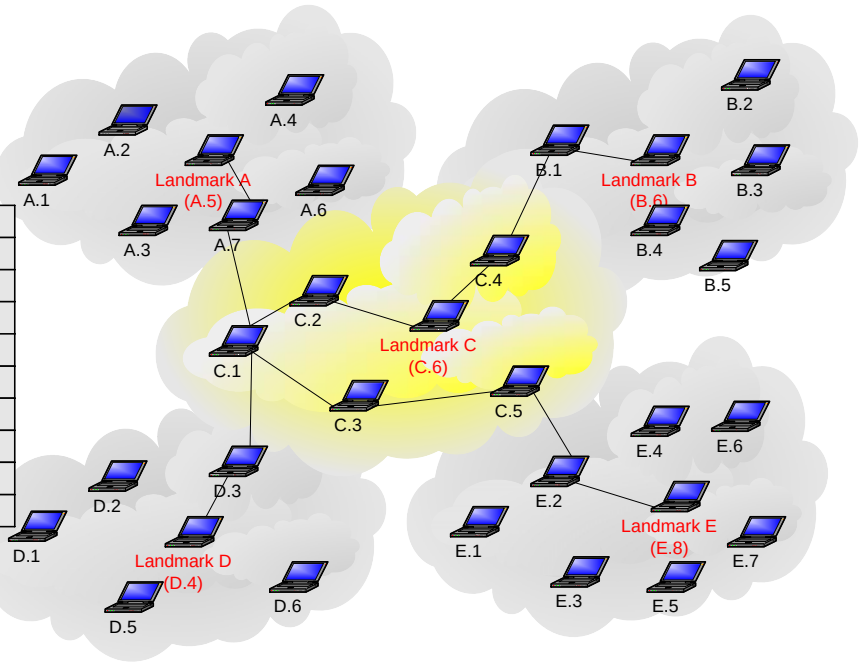

Figure 3.1.1 Landmarks and LANMAR Group Routing

Figure 3.1.1 illustrates a MANET with five logical groups A, B, C, D, and E. Node C.1 belongs to group C. Node C.1 knows how to send a packet to any of its group members C.2, C.3, C.4, C.5, C.6. The routing table of node C.1 shows that there is a routing entry for each of its group members. However, if node C.1 needs to deliver a packet to node E.7, node C.1 sends it to landmark E instead of the destination E.7 because node C.1 does not have a route entry for E.7 in its routing table. Node C.1 only knows that it can reach landmark E by sending the packet to node C.3 as we will explain in a later section. The landmark E represents its group members to outside nodes. Packets destined to any members of group E will be first directed to landmark E.

LANMAR introduces the concepts of landmark and logical groups. It differentiates the routing scheme within a logical group and between logical groups. The routing scheme within a logical group is described as in-scoped routing in Section 3.1.1.1. The out-scoped routing is explained in Section 3.1.1.2. Finally, Section 3.1.1.3 and Section 3.1.1.4 discuss landmark election and drifter nodes.

3.1.1.1 LANMAR In-scoped Routing

In-scoped routing protocol is also called a host protocol. Currently, the LANMAR implementation employs Fisheye State Routing (FSR) as the in-scoped routing protocol. The eye of a fish captures with high detail the pixels near the focal point. As the distance from the focal point increases, the detail decreases. In routing, the fisheye approach is translated to maintaining accurate routing information (distance and path quality) about the immediate neighborhood of a node, with progressively less detail as the distance increases. FSR is a proactive link state based routing protocol in which topology information is disseminated in a different way than most link state routing protocols. A node maintains a link state table based on the up-to-date information received from neighboring nodes, and periodically exchanges it with its local neighbors instead of flooding its link state to the entire network. The key difference is the way that the link state is propagated periodically. By several exchange periods, a full topology map is received and kept at each node and shortest paths are computed based on the full topology map.

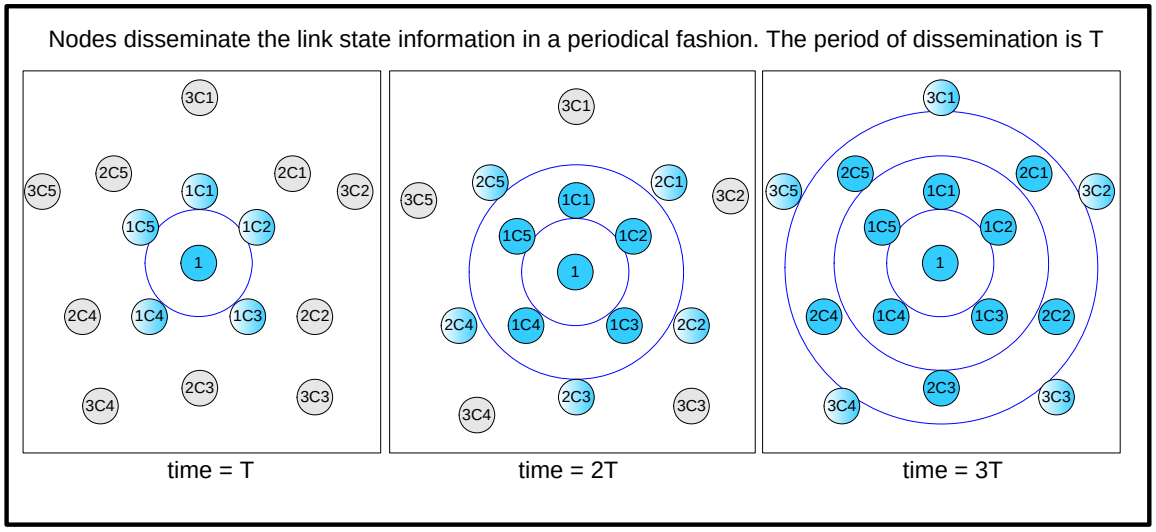

Figure 3.1.2 Link State Information Propagation in a Periodical Fashion

Figure 3.1.2 illustrates the periodical dissemination of link state information. At the first period, node 1 exchanges link state information with its neighbors. Node 1C1, 1C2, 1C3, 1C4, 1C5 receive the link state of node 1 at time T. Instead of forwarding the link state immediately, node 1C1, 1C2, 1C3, 1C4, 1C5 wait for the second propagation period. At the second propagation period, node 1C1, 1C2, 1C3, 1C4, 1C5 exchange their link state information with their one-hop neighbors as well as forwarding their one-hop neighbors' link state information. Node 2C1, 2C2, 2C3, 2C4, 2C5 receive the link state information of node 1 at time 2T. By using the same procedure, node 3C1, 3C2, 3C3, 3C4, 3C5 receive the link state information of node 1 at time 3T. Each node progressively slows down the update rate for destinations as

their hop distance increases. Entries corresponding to nodes within a smaller scope are propagated to neighbors with a higher frequency. As a result, a considerable fraction of topology table entries (corresponding to remote destination) are suppressed in a typical update, thus reducing the bandwidth utilization.

This approach produces accurate distance and path quality information in the immediate neighborhood of a node, with progressively less detail as the distance increases. As a packet approaches its destination, the route becomes more precise.

LANMAR routing distinguishes the routing scheme inside a logical group and between logical groups. Nodes inside a logical group know the exact routes to other members in the same group by using the FSR mechanism.

3.1.1.2 LANMAR Out-scoped Routing

Each logical group has one node serving as a landmark. All the MANET nodes need to build routes to landmarks no matter whether they are in the same logical group with the landmark or not. The distance vector routing scheme is used to disseminate the routes to landmarks. A distance vector gives the landmark network address and the sending node's distance expressed in hops to the landmark. This information is disseminated to the whole network. A message type: LANMAR Update (LMU) is used to carry the distance vector. The LMU messages are periodically exchanged with neighbors to propagate the routing information to the landmark nodes. The size of the landmark distance vector is equal to the number of logical subnets and thus to the landmark nodes. When a node receives a distance vector from a neighbor node and finds that the neighbor node has shorter distance to some landmark nodes, the node will recalculate its routing table as well as update its distance vector table. Then, the node will propagate the distance vector to all landmarks based on its current distance vector table in the next propagation period. Every node receives and keeps the link state for all nodes within its logical group using the FSR (the in-scoped routing) while maintaining a distance vector of all the landmarks for all logical groups.

LANMAR combines the features of FSR and Landmark Routing. After the logical group and the landmark is introduced, the main difference between LANMAR and FSR is that FSR routing table contains "all" nodes in the network, while the LANMAR routing table includes only the nodes within the fisheye scope (expressed in number of hops) and the landmark nodes. This feature greatly improves scalability by reducing routing table size and update traffic overhead. The restriction is that all nodes in the same logical group have to be assigned addresses that reflect their group membership or otherwise have to be identified as a member of the same group through other means.

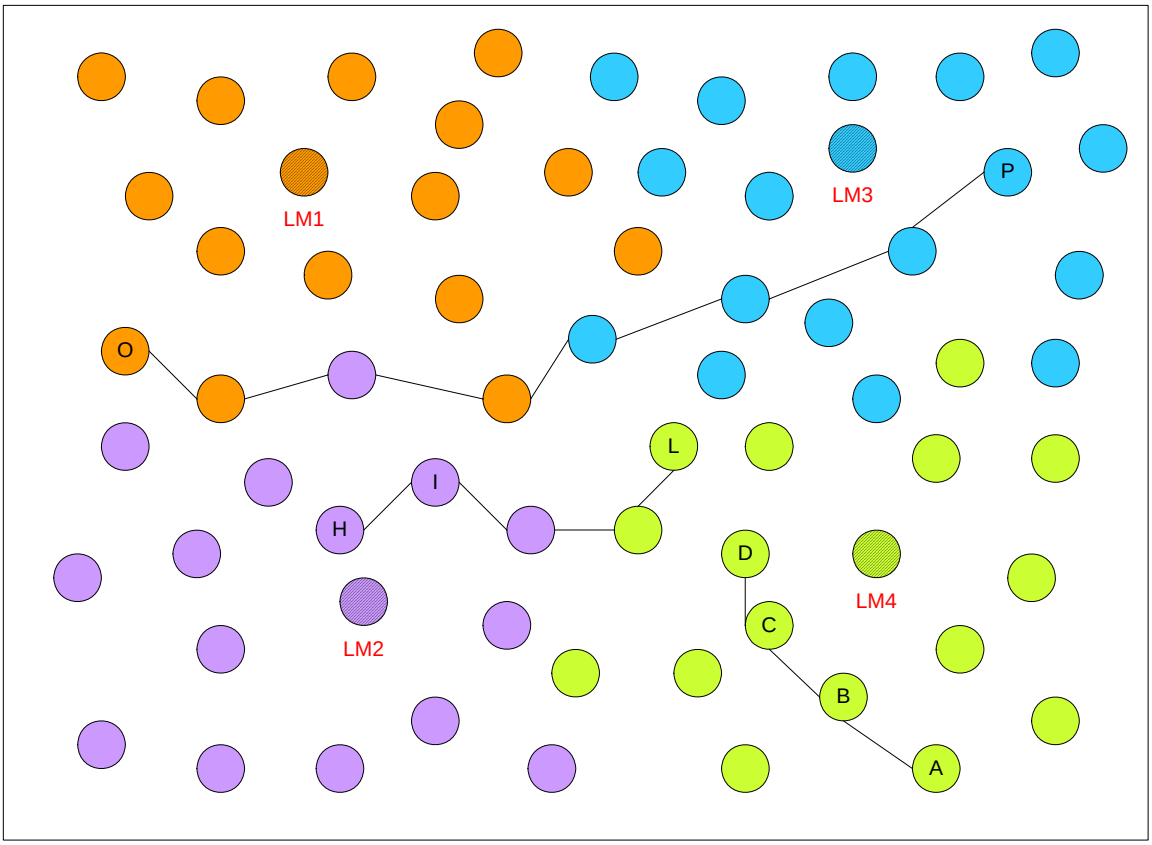

Figure 3.1.3 An Illustration of LANMAR Routing

Figure 3.1.3 is an example of LANMAR routing inside a group and between groups. There are four logical groups in the MANET and each group has its landmark node LM_1, LM_2, LM_3, LM_4. The radius of the fisheye scope is 2. Inside the group, routes are created by the FSR routing. Outside the group, the routes to landmarks LM_1, LM_2, LM_3, LM_4 are built by propagating a LMU message. The first path is from node A to D. C is within the fisheye scope of node B; thus, B will propagate the link state of node C, indicating D as a neighbor. Then node A has the complete routing information about D and can deliver the packets along the shortest path to D. The second path is from H to L. H does not have the route to L. It routes the packets towards the landmark of node L (LM4) throught I. Node I does have the route to L because L is within its fisheye scope and can forward the packets directly using the shortest path instead of the landmark LM4. A third, much longer path (from O to P) is also shown. The path leads first to the landmark (LM3) of node P. As the packet approaches LM3, it obtains the direct route to P. It thus bypasses LM3 and reaches P.

3.1.1.3 Landmark Election

All group members participate in electing a landmark node. At the beginning, no landmark exists in a logical group. From the in-scoped routing protocol FSR, a node will learn how many nodes are in its fisheye scope. By comparing the number of nodes with a predefined number, it declares itself as a landmark if there are enough nodes in its fisheye scope. Neighbor nodes exchange the landmark declaration information by using LMU message. Landmark declaration information is a status pair containing the ID of the landmark and the number of group members it can reach within the FSR scope. When more than one node declares itself as a landmark in the same group, the node with the largest number of group members wins the election. In the case of a tie, the lowest ID breaks the tie. Prior to landmark election, a logical group needs to be defined. High mobility and dynamic membership are challenges to landmark selection. If frequent landmark re-election happens, the network will be in a transition state. During the transition period, there is large packet loss. If LMU packets are still propagated in period, the network's reaction to the topology change will be slow. If LMU packets are exchanged fast, overhead increases. The LANMAR protocol may lose the advantage gained from the landmark feature.

3.1.1.4 Drifter Nodes

Routing to any nodes in a logical group aims to its landmark. This requires that the landmark of each subnet should have a route to all members in a logical group. However, it is normal that some of members "drift off" outside the fisheye scope of landmark node because of a MANET node's mobility nature. To make the route to such "drifters" known to a landmark, the following modification to the routing table exchange is necessary.

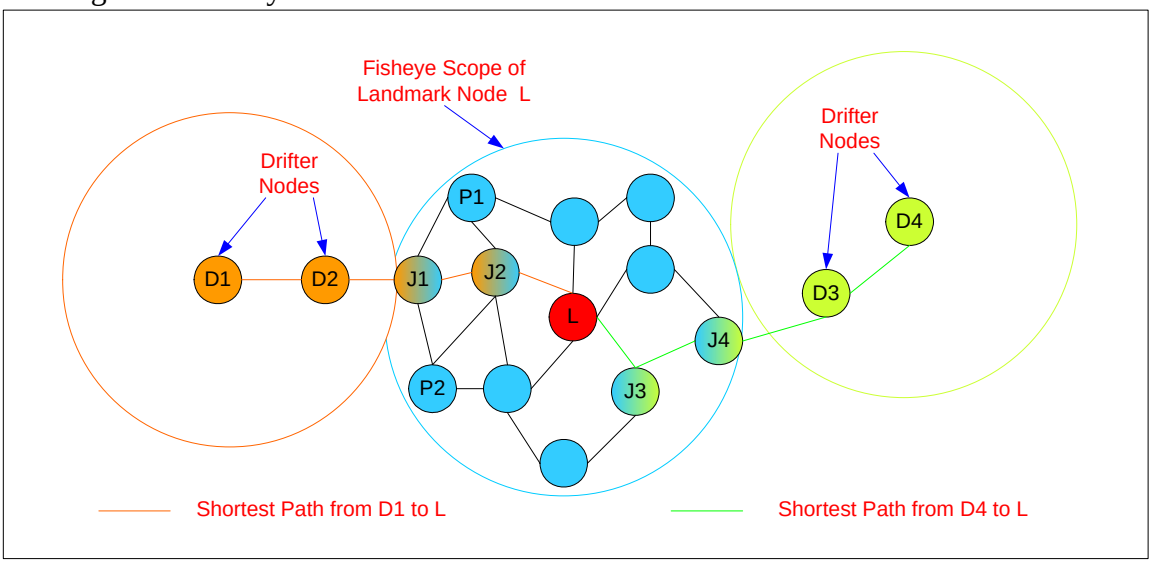

Figure 3.1.4 Shortest Path from Drifter Nodes to Landmark Node

Figure 3.1.4 shows a logical group where the landmark is node L. The fisheye scope is two hops. D1, D2, D3, and D4 receive the LMU and know they are out of the landmark's fisheye scope because the LMU message indicates the distance to the landmark (i.e. three or four hops). Drifter nodes know how to route a packet to their associated landmark by receiving the landmark distance vector. However, the reverse path (route from landmark to the drifter) is not known by landmark. To make the landmark know how to route a packet to the drifters, a new distance vector, called the drifter for distance vector (DFDV), is propagated along the shortest path from landmark to the drifter nodes. A drifter node sends a DFDV to its neighbor nodes. A node, say i, on the shortest path between a landmark L and a drifter D associated with such landmark keeps a distance vector entry to D. If D is within FSR scope of node i, this entry is already included in the FSR table of node i. When i transmits its distance vector to neighbor j, then j will retain the entry for member D only if d (j, D) < scope or d (j, L) < d (i, L). The latter condition occurs if j is on the shortest path from i (and therefore from l) to L. In the example, D1 sends DFDV to D2. Node D2 keeps a distance vector entry to D1 because d (D2, D1) < scope. D2 retransmits the DFDV to its neighbors. Node J1 keeps a distance vector entry to D1 because d (J1, D1) < scope. When J1 transmits the D1's DFDV to its neighbors P1, P2, and J2, only J2 will retain the entry for node D1 because d (J2, L) < d (J1, L). J2 is actually on the shortest path from J1 (and therefore from D1) to L. This way, a shortest path is built from the landmark to its drifter node D1. Using the same method, the shortest paths are maintained from the landmark L to each one of its drifters D1, D2, D3, D4.

3.1.2 Hierarchical LANMAR

The original LANMAR scheme is suitable for large-scale flat networks. When it is applied to a hierarchical structure like the proposed military tactical scenario presented in this report, LANMAR needs to be extended into a hierarchical routing protocol.

A hierarchical structure where the Hierarchical LANMAR (H-LANMAR) works is demonstrated in ***Figure 3.1.5***. The ordinary ground nodes with limited short transmission range are divided into groups. Each group has one backbone node. These backbone nodes have an additional, powerful radio and can form a higher- level backbone network. UAVs can further be used to connect the backbone.

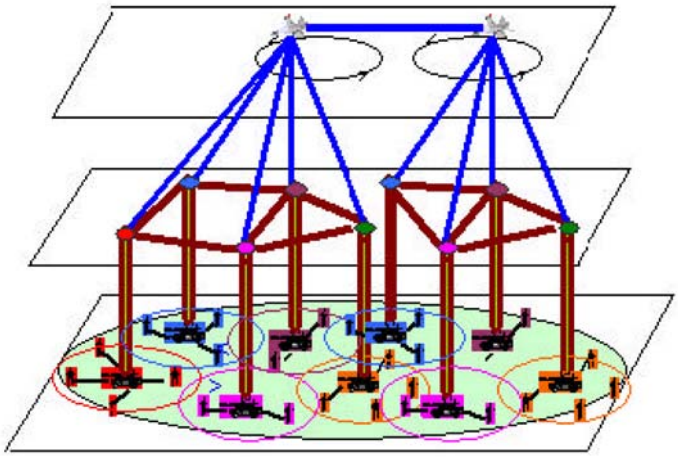

Figure 3.1.5 Multi-level Hierarchical Ad Hoc Network

H-LANMAR can be well integrated into UAV based hierarchical structure. In the original LANMAR scheme, while routing packets to remote nodes, the packet is routed toward the corresponding remote landmark along a long multi-hop path. In the hierarchical structure, we can route the packet to a nearby backbone node. Then the backbone node can forward the packet to a remote backbone node near the remote landmark through the higher-level links. The remote backbone node can then send the packet to the remote landmark or directly to the destination. This will greatly reduce the number of hops. To take the "shortest route", the H-LANMAR extends the original LANMAR routing protocol as follows: First, all nodes, including ordinary nodes and backbone nodes, will still run the original LANMAR routing using the short-range ground radios. Second, a backbone node with a longer-range radio will broadcast the landmark distance vectors to neighbour backbone nodes via backbone links, and even to UAVs. The content of this packet is the same as the original landmark update packet. The neighbour backbone nodes will treat this packet as a normal landmark update packet. Since this higher-level path is usually shorter, it will replace the longer multi-hop paths. From landmark updates the ground nodes thus learn the best path to the remote landmarks, including the paths that utilize the higher-level links. To route packets using the correct radio interface, each backbone node needs to remember the radio interface to the next hop on each path.

3.1.3 H-LANMAR Benefits and Issues

H-LANMAR decreases the routing table size as well as reduces the update message overhead by using landmark nodes. It is suitable for pure group mobility without inter-group movement activities.

H-LANMAR faces the problem of the drifting node. A node that moves to another group is a drifting node. The routing to a drifting node in H-LANMAR needs special

treatment since H-LANMAR relies on a hierarchical addressing scheme. If many nodes move between groups, a large number of drifting nodes will cause high overhead and no optimized routes. Routing to an isolated node that moves into another group is difficult to handle. In a highly dynamic and mobile environment, landmark nodes may shift frequently and the fraction of drifting nodes may be large. The transient behavior can result in inconsistent routing tables and may cause packet losses and longer routing paths. Landmark distance vectors are propagated slowly to the whole network because the LMU messages are periodically exchanged between local neighbor nodes as opposed to being flooded in the network. It takes n*(exchange intervals) time for an n-hop away node to notice the change of a landmark. Reaction to the topology change will be very slow in a highly mobile network. It may seriously decrease the performance of the protocol.

In the LANMAR draft and related papers, there is no clear description of how to handle the scope redefinition and landmark election issues when two logical groups merge together. Fisheye scope is employed to reduce the size of update messages in FSR routing. Normally, several scopes are defined to achieve graded update rates. LANMAR handles routing within a logical group by the FSR while handling routing outside a logical group by LMDV distance vector. The concept of logical scope is different from the fisheye scope. In the draft and related papers, no clear declaration is presented about the difference. According to our understanding, the logical scope of a group has been implicitly set to the fisheye scope of the landmark node of the group. An effective method for the selection of the size of the logical scope is never discussed in the LANMAR draft and related papers.

3.2 H-OLSR

3.2.1 Introduction to OLSR

OLSR is a proactive protocol for mobile ad hoc networks. The OLSR protocol is a variation of the pure link state routing (LSR) protocol and is designed specifically for MANETs. The OLSR protocol achieves optimization over LSR through the use of MPR (Multi Point Relay) nodes. The MPR nodes are selected and designated by neighboring nodes. Unlike LSR, where every node declares its links, only MPR nodes declare links. Also, unlike LSR, where each node forwards messages for their neighbors, only MPR nodes forward messages for those neighbor nodes that selected them as a MPR node.

Each node selects its MPR set of nodes in a way that, through them, it can reach all of its two-hop neighbors. A node learns about its one-hop and two-hop neighbors from its one-hop neighbors' HELLO messages. By exchanging HELLO messages, a node finds out which neighbors have chosen it as a MPR. The neighbors that select a node as MPR form that node's MPR Selector set. A TC (Topology Control) message

is sent periodically by each MPR in the network to declare its MPR selector set and is used in the construction of routing tables.

3.2.2 H-OLSR

The H-OLSR [6][7] model is based on the protocol specifications for the OLSR algorithm. H-OLSR dynamically organizes nodes into cluster levels. The cluster structure supports random movement of the nodes and has diagnostic capabilities.

3.2.2.1 H-OLSR Logical Topology Levels

The proposed network architecture for the H-OLSR is illustrated in ***Figure 3.2.6***. Based on the different components in the network, the nodes are organized into multiple logical topology levels. The low-power nodes, designated by circles, are equipped with only one interface offering limited data rate and transmission range. Such nodes participate at the topology Level 1, and can represent rescue personnel whose communications are constrained by the limitations of the communications equipment these individuals can carry.

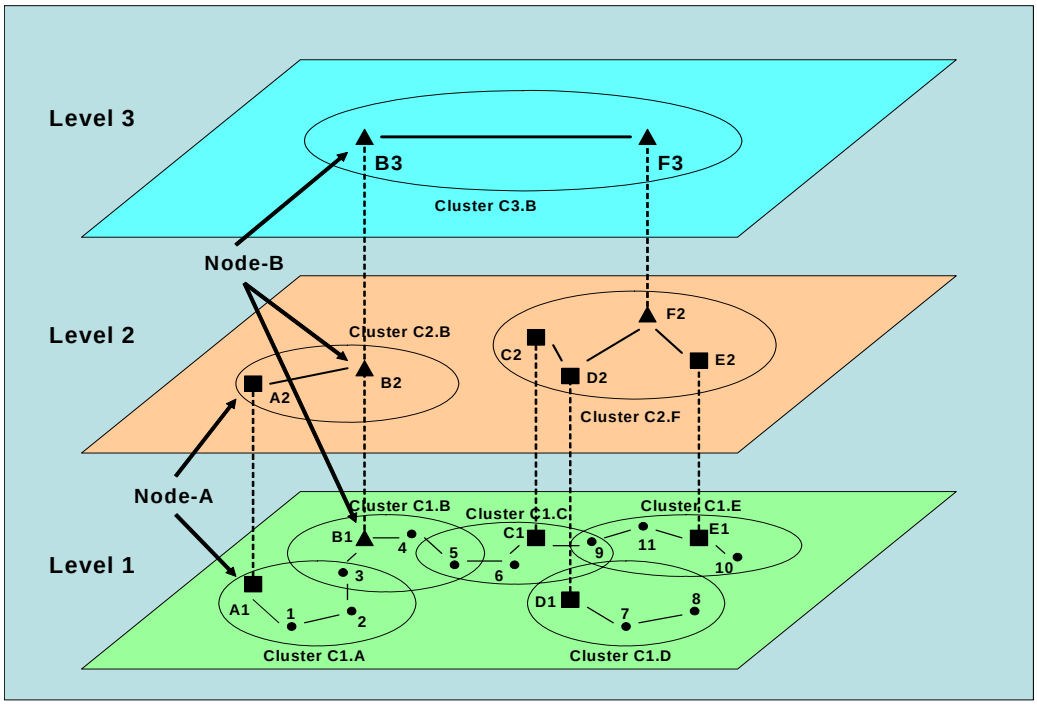

Figure 3.2.6 An Example of Heterogeneous Network

Nodes at the topology Level 2, designated by rectangles, are equipped with two interfaces, one of which is a wireless interface capable of communicating with Level 1 nodes. These mobile nodes can also relay messages at the logical topology Level 2 using a frequency-band or a medium-access control (MAC) protocol, which differs from the one, used for communication at the topology Level 1 – this additional wireless interface affords a longer transmission range than the one used by Level 1 nodes. Such nodes can represent mobile units such as ambulances and police forces, capable of communicating with individual personnel as well as with other mobile units on different frequency bands.
Topology Level 3 nodes, designated by triangles, can represent helicopters. These nodes are equipped with three wireless interfaces capable of communicating in turn with Level 1 (not mandatory) and Level 2 nodes, and with other Level 3 nodes via high-speed point-to-point direct wireless links.

At each logical topology level, nodes form clusters, select MPRs, and exchange network topology information independently. Unlike the original (flat) OLSR, which transmits the same topology control information from all interfaces, in H-OLSR each interface sends out topology information relating only to its own level. In actuality these interfaces run H-OLSR independently as individual nodes.

The elements in ***Figure 3.2.6*** are designated as follows: Clusters are labeled by an uppercase '**C**' (denoting 'Cluster'), followed by a digit indicating the topology level at which the cluster is grouped, followed in turn by an uppercase letter indicating which node functions as cluster head. Thus for example, **C2.B** designates a Level 2 cluster having node **B** as cluster head, etc. Nodes are designated in one of two ways, depending on whether they are single-interface or multiple-interface nodes, as follows: Nodes indicated by small **CIRCLES** possess only one interface, and each such node is represented by a single digit (**1**, **2**, **3**, etc.); these nodes are found only at the bottom level. Multiple-interface nodes, which operate on multiple topology levels, are represented by two characters: an uppercase letter designating the node's *name* (**A**, **B**, **C**, etc.) followed by a digit indicating the node's *interface*, the digit corresponding to the topology level at which that interface operates. Nodes with interfaces indicated by **TRIANGLES** can operate at each of the three levels (viz: **B3**, **B2**, **B1**), while nodes with interfaces indicated by **SQUARES** operate at only the lower two Levels (viz: **E2**, **E1**). Please note: in reality, nodes do not always follow strictly the interface guidelines outlined above. For instance, topology Level 3 nodes could conceivably possess only two interfaces: one to communicate with peers in Level 3, and the second to communicate with nodes in Level 2 below. This is exemplified by **node F** in our illustration, which is a Level 3 node possessing only two interfaces.

3.2.2.2 H-OLSR Cluster Formation

Mobile nodes form different cluster levels, a cluster being comprised of a group of mobile nodes (at the same topology level) having selected a common cluster head. Clusters are self-organized, with cluster heads being configured during the start-up of

the H-OLSR process, whereby any node participating in multiple topology levels automatically becomes the cluster head of any lower-level nodes. In the above example, node **A**, which participates in both topology Levels 1 and 2, can become the Level 1 cluster head, while **B**, which participates in topology Levels 1, 2 and 3, can become the cluster head at both Level 1 and Level 2.

At each level the cluster head declares its status and invites other nodes to join its cluster by periodically sending out Cluster ID Announcement (CIA) messages (these are sent together with the Hello messages to reduce the number of packet transmissions). CIA messages contain two fields: *cluster head*, which identifies the interface address of the cluster head selected by the message generator, and *distance* (in hops) to that cluster head. When a cluster head generates a CIA message, it identifies itself within the *cluster head* field, with *distance* being 0. The nodes in proximity to the cluster head receive the CIA messages, join the cluster, and begin generating CIA messages inviting nodes further away to join the cluster. Any given node may receive two or more CIA messages, indicating that it is located in the overlapping regions of several clusters. In such cases, the node joins whichever cluster is closest in terms of the hop count. For instance, in our example *interface* **A1** of *node* **A** sends out the following CIA message: "*cluster head*: A1; *hop count*: 0". The CIA message is received by **A1**'s next-hop neighbor, node **1**, who then joins cluster **C1.A** and generates a CIA message: "*cluster head*: **A1**; *hop count*: 1", which is received by node **2**. Therefore, node **2** also joins cluster **C1.A**. Node **3**, which is in the transmission range of both **2** and **B1**, receives two CIA messages: one from **2** indicating: "*cluster head*: A1; *hop count*: 2", and one from **B1** indicating: "*cluster head*: B1; *hop count*: 0". In this case, node **3** chooses to join the closer cluster **C1.B,** managed by **B1**. Following this process, each Level 1 node joins a selected cluster, and the mechanism is in turn applied at each respective topology level. It should be noted that given the random movement of the mobile nodes, a node might find a cluster head that is closer than the one to which it is currently attached. In this case, the mobile node will proceed to change its cluster and attach itself to the closest cluster head.

A built-in diagnostic feature helps ensure the robustness of H-OLSR's clustering mechanism: as CIA messages are generated, each node monitors the time-out value of the CIA messages received. Should a cluster head become inactive or move away, no CIA message is received after a period of time and the original CIA information becomes invalid. The node can then accept a CIA message from another cluster and will join that cluster should the opportunity present itself. As per our example, suppose **B1** goes down; after **B1**'s CIA has timed out, **3** can join cluster **C1.A** when it receives the CIA message from **2**; **5** joins cluster **C1.C** upon receiving the CIA message from **6**; finally, **4** also joins cluster **C1.C** when receiving the CIA message from **5**, after **5** has joined **C1.C**. The clusters are therefore automatically reconfigured. If no CIA messages are received, that is, if the network is no longer heterogeneous and is comprised of nodes having only a single interface (i.e., there are no longer any

multiple-interface nodes in the network), the H-OLSR treats the entire network as one cluster, and behaves as would the original OLSR.

3.2.2.3 Cluster Message Exchange

3.2.2.3.1 Cluster Head Message Exchange

In H-OLSR, a cluster head acts as *gateway* through which messages from cluster members are relayed to other parts of the network; therefore each cluster head needs to be aware of the membership information of its peer cluster heads. A Hierarchical Topology Control (HTC) message is used to transmit the membership information of a cluster to the higher hierarchical level nodes. Three basic types of HTC messages are used: the *full membership* HTC message, the *update* HTC message and the *request* HTC message. The *full membership* HTC messages are periodically transmitted by a cluster head to provide information about its cluster members, including members of any lower-level clusters beneath it. The *update* HTC messages provide information with respect to cluster membership changes, that is, the *update* HTC messages are used when mobile nodes join or leave a cluster. As HTC messages carry a sequence number field, it is possible to determine whether any HTC packet loss has occurred, in which case a *request* for the re-transmission of *a full membership* HTC message is sent by the receiving node. HTC forwarding is enabled by MPRs, and is restricted within a cluster. As per our example, node **A**, which is the cluster head of Cluster **C1.A**, generates HTC messages from *interface* **A2** informing other Level 2 nodes that **1**, **2** and **A1** (itself in Level 1) are members of its cluster. **B**, which is the cluster head of Cluster **C2.B**, generates HTC at topology Level 3, advertising that **1**,**2**,**3**,**4**,**5**,**A1**,**B1** (at topology Level 1) and **A2**,**B2** (at topology Level 2) are members of its cluster. **A**'s Level 2 HTC is relayed to other Level 2 nodes within Cluster **C2.B**; **B**'s Level 3 HTC is relayed to other Level 3 nodes.

In topological terms, the higher a given node is located, the more information it obtains about the network. Nodes at the highest topology level possess full knowledge of all nodes in the network; consequently the sizes of their routing tables are as large as they would be under OLSR. However, because the topology information required by lower-level nodes is limited in scope, the sizes of their routing tables are consequently reduced as compared to the original (flat) OLSR.

3.2.2.3.2 Topology Control Message Propagation

H-OLSR clustering does not require nodes at each hierarchical level to independently select MPRs in their respective cluster level: in the above example, nodes in Cluster **C1.A** select MPRs at Level 1, while nodes in Cluster **C2.B** select MPRs at Level 2. At each hierarchical level, TC messages are generated independently. The propagation of the TC is usually restricted within a cluster, unless

a node is located in the overlapping regions of several clusters. For example, **2** in Cluster **C1.A** may accept a TC from **3**, which is in Cluster **C1.B**, and forward it to **1**. However, **1** retains only the information relating to that TC, without passing it on. Therefore, an H-OLSR node's *location* directly determines the required scope of its knowledge of network topology: for nodes located towards the center of the cluster, TC propagation is limited to the local cluster; for nodes located in the overlapping regions of multiple clusters, the TC message is propagated not only within the local cluster but to neighboring clusters as well. This approach offers two main advantages: 1) the control message reflecting local movement is restricted within the local area, which largely reduces protocol overhead as well as routing-table computation overhead; 2) nearby nodes in different clusters at the same level can communicate directly without having to follow the strict clustering hierarchy, which decreases delay and reduces the load on the cluster head.

3.2.2.4 Data Transfer

For data transmissions outside the local area, the employed gateway mechanism can be illustrated as follows: node **1**, which is a member of Cluster **C1.A**, intends to send data to node **10**, which is in Cluster **C1.E**. From Hello and TC messages, node **1** knows that node **10** is not a member of its cluster, so it sends data to its cluster head **A**. Node **A** in turn does not recognize node **10** as a member of its cluster, nor does it see node **10** from the TC or HTC messages (which convey only the topology or membership information within Cluster **C2.B**), therefore node **A** relays the data packet to its cluster head **B**. Cluster head **B** in turn knows from the HTC message originated by node **F** (which is within its Level 3 cluster) that node **10** is a member of node **F**'s cluster, therefore the data packet is relayed to node **F**, and finally to its intended destination node **10** via node **E** (which is the cluster head where **10** is located). As we trace the transmission route traveled by the data packet (1→ A → B → F → E→10), we see that the cluster head is always used as the gateway by member nodes at lower hierarchical levels when transmitting to destinations outside the local area. However, when data are transmitted between neighboring nodes, the cluster head is not involved even though the nodes may belong to different clusters. In the case of node **2** (member of cluster **C1.A**) transmitting data to **B1** (member of cluster **C1.B**), the data packet is directly relayed to **B1** through **3**, as **2** knows that it can reach **B1** via **3** from **3**'s TC (see the above discussion outlining how a node accepts the TC from other clusters.) With this strategy, H-OLSR makes efficient use of high capacity nodes without overloading them.

3.2.3 H-OLSR Benefits and Issues

The main improvements realized by the H-OLSR protocol are a reduction in the amount of topology control information that needs to be exchanged at different levels of the hierarchical network topology, and the efficient use of high capacity nodes. Another significant benefit is a reduction in routing computational cost: if a link in

one part of the network is broken, only those nodes within that cluster need to re-calculate the routing table, while nodes in other clusters are not affected. More importantly, H-OLSR is versatile in that it does not require a logical addressing scheme but can accommodate one if required. Unlike most routing protocols for large scale MANETs such as LANMAR are restricted in hierarchical addressing structures, the logical hierarchical addressing scheme is not necessary for H-OLSR.

H-OLSR can be directly applied to the network structure shown in ***Figure 2.1.1***. The nodes equipped with high capacity links form the higher-level network, while the nodes with low capacity links form the lower level network. Nodes (including tanks, APVs, soldiers) can move from one group to another and associate with the nearest higher capacity nodes (cluster heads), while the cluster heads propagate updated membership information using HTC messages.

According to H-OLSR's network structure, a higher-level cluster should have a higher bandwidth capacity compared to its lower layer to optimize H-OLSR's performance. Because packets often travel through cluster heads (high layer) instead of the nodes in the same layer if clusters exist, it means that more traffic will go through the cluster head. If cluster heads do not have higher capacity links, they become bottlenecks for their clusters.

4. Performance Comparison of H-OLSR and H-LANMAR

4.1 NS2 Simulation Setup

4.1.1 Protocol Implementation

NS-2 is used as a simulation tool to evaluate and compare the performance of the two proactive hierarchical routing protocols discussed in the previous section. The original NS-2 implementation only supported a single interface capability. CRC extended the NS-2 implementation to support multiple interfaces, where each interface can be configured to support different transmission ranges and data rates.

CRC also implemented and integrated H-OLSR into the extended NS-2 implementation. The original LANMAR implementation was provided by UCLA in the GLOMOSIM simulator. That implementation was ported by CRC from GLOMOSIM to NS-2 and was extended to support the H-LANMAR features as well.

4.1.2 Network Setup

The general layout of a heterogeneous network is simulated. The network occupies a 1200m x 1200m flat space, and contains 90 mobile nodes. These are divided into 9 groups, where each group consists 10 mobile nodes. In each group, there is a backbone node equipped multiple interfaces, while others are equipped with only one wireless interface (interface 0). For the 9 backbone nodes, 4 of them have 2 interfaces (interface 0 and interface 1) while the remaining 5 have 3 interfaces (interface 0, interface 1 and interface 2).

The physical layer on the interfaces at all hierarchical levels is IEEE 802.11. Interfaces function in fixed rate mode (no rate fallback or autobaud). To simulate higher capacity links (with longer transmission range and higher data rate) the following method is used: a fixed raw data rate of higher value is selected, and the (fixed) transmission power is adjusted accordingly, in order to have a higher transmission range. It is also assumed that the frequency bands of the interfaces are carefully selected such that an increase in transmission power will not cause increased interference with other interfaces. The specification of each interface is presented below.

- Interface 0 – data rate 2Mbps, transmission range 200m. All mobile nodes, including the backbone nodes, are equipped with interface 0. The nodes that are equipped with only interface 0 are level 1 nodes.

- Interface 1 – data rate 5Mbps, transmission range 450m. All the backbone nodes are equipped with interface 1 on top of their interface 0. Among them, 4 of the backbone nodes only have 2 interfaces. Those nodes are level 2 nodes.
- Interface 2 – data rate 11Mbps, transmission range 2000m. 5 of the backbone nodes are equipped with interface 2, in addition to their interface 0 and interface 1. Those nodes are level 3 nodes.

4.1.3 Movement Pattern

To create node movement, we used both the mobility scenario generation tool, BonnMotion and the NS-2 provided random waypoint mobility scenario generator. 4 movement patterns are used to compare and analyze the performance of H-LANMAR and H-OLSR: Strict Internal Group Motion pattern, Internal Group Motion with Drifting Nodes pattern, Group Moving pattern, and Group Merging pattern. The detailed setup of each movement pattern will be presented in section 4.2.

4.1.4 Comparison Metrics

Three metrics are used to compare the performance of H-OLSR and H-LANMAR: normalized routing message overhead, packet delivery ratio, and end-to-end delay. The definitions of the three metrics are given in the following sections.

4.1.4.1 Normalized Routing Overhead

It is defined as the ratio of the number of routing packets transmitted to the number of data packets actually received.

$$NormalizedRoutingOverhead = \frac{numberOfSentRoutingBytes}{numberOf\ \mathrm{Re}ceivedDataPackets}$$

This metric shows how efficient a routing protocol is. A high value of normalized routing overhead indicates that more bytes of routing packets are sent in terms of a received data packet and consequently lower the efficiency of the protocol.

As mentioned in the previous sections, H-OLSR routing packets consist of four types: Hello message, TC message, CIA message and HTC message. A Hello message identifies a node itself and reports a list of its neighboring nodes. A TC message identifies the source node as an MPR node and announces those nodes that have selected this node as their MPR. A CIA message declares a node as cluster head. A HTC message is used to transmit the membership information of a cluster to the higher hierarchical level nodes [6]. H-LANMAR routing packets include two types of messages: FSRL (Fisheye Routing Link State) message and LMU (LANAMR) update message. A FSLR message identifies a node itself and reports its topology table

within a predefined fisheye scope, while a LMU message announces a node's knowledge of all landmarks and its distances to all landmarks.

For the all simulations, in H-OLSR, the HELLO interval is set to 2 seconds, while the TC and HTC intervals are set to 5 seconds. Similarly, in H-LANMAR, the FSRL interval is 2 seconds, the LMU interval is 5 seconds and the fisheye scope is 2.

4.1.4.2 Packet Delivery Ratio

It is calculated as the ratio between the total numbers of data packets successfully received by the destination nodes to the number of data packets sent by the source nodes during the time period of the simulation.

$$PacketDeliveryRatio = \frac{numberOf\ \mathrm{Re}ceivedDataPackets}{numberOfSentDataPackets}$$

This metric represents how successful the protocol is in delivering packets to the application layer. The higher the packet delivery ratio is, the more data packets are being delivered to the higher layers. Under the same network conditions, a better packet delivery ratio with a routing protocol indicates that this routing protocol has a better performance.

4.1.4.3 End-to-End Delay

It is calculated as the average delay in transmission of a packet from a source node to a destination node. It is defined as follows:

$$End-to-EndDelay = \frac{\sum_{i=0}^{n}(timeOfDataPacket\ \mathrm{Re}ceived_i - timeofDataPacketSent_i)}{totalNumberOfDataPacket\ \mathrm{Re}ceived}$$

A higher value of end-to-end delay indicates that the network is congested which is either caused by too much data traffic load or caused by high routing packets overhead. The upper bound of end-to-end delay value is determined by the application. FTP traffic or web surfing can tolerate high end-to-end delay value. However, voice and real time audio and video traffic cannot tolerate high end-to-end delay value.

4.2 Simulation Results

In this section, H-OLSR and H-LANMAR are compared under four distinct movement patterns – the Internal Group Motion pattern, the Internal Group Motion with Drifting Nodes pattern, the Group Moving pattern, and the Group Merging

pattern. In each of the movement patterns, node speed is set to 10m/s, and nodes move continuously without stopping. Different network loads are applied to each movement pattern to observe the performance of the routing protocol. The specification of network load is defined in ***Table 4.2.1***. The simulation time is 600s for all simulations. Results of the normalized routing overhead, the packet delivery ratio and end-to-end delay of H-LANMAR and H-OLSR are presented, summarized and analyzed for each of the movement patterns.

Traffic Pattern	**Light Traffic**	**Medium Traffic**	**Heavy Traffic**
Number of Connections	20	40	60
Payload Size	64 bytes	256 bytes	512 bytes
Packet Rate	4 packets/sec	4 packets/sec	4 packets/sec

Table 4.2.1 Traffic Patterns For The Scenarios

4.2.1 The Internal Group Motion Pattern

4.2.1.1 Movement Pattern Description

In the Internal Group Motion pattern scenario, each group has its own fixed location. A group will not move to other locations during the simulation period. However, nodes that belong to a group randomly move inside their group's local area. The Random Waypoint mobility model [10] is used to generate the movement of a node when a node moves inside the area of its own group. The parameters defined for this scenario are as follows:

Parameters	**Values**
Mobility model	A group stays in a fixed location Nodes randomly move inside a group (Random Waypoint mobility model with max speed of 10m/s, min speed of 0m/s, no pause time)
Distribution of nodes	10 nodes in each group 9 groups
Global simulation area	1200m * 1200 m
Local area of a group	200m*200m

Table 4.2.2 Parameters for The Internal Group Motion Pattern

4.2.1.2 Normalized Routing Overhead

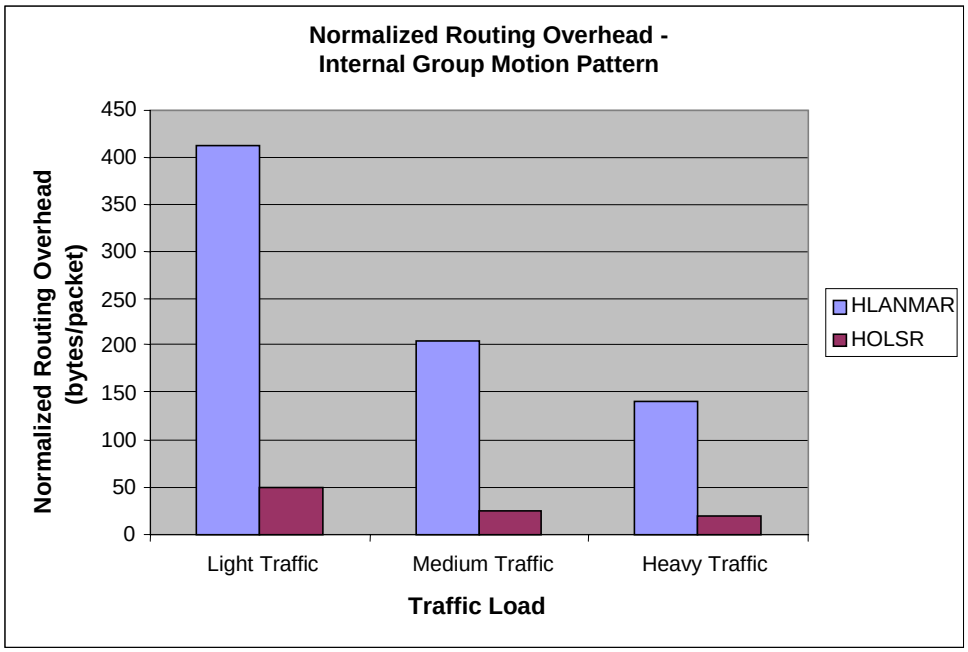

Figure 4.2.1 Normalized Routing Overhead Under Different Traffic Loads for Internal Group Motion

Control Overhead: When Internal Group Motion pattern is applied in the network, H-OLSR always has much lower overhead than H-LANMAR. This is because the control messages in H-OLSR are much shorter than that in H-LANMAR – the FSRL messages in H-LANMAR consists of the fisheye scope topology table of a node. When nodes exchange the FSRL message, the link state information of all the nodes in the fisheye scope are exchanged. As the fisheye scope is set to 2 [4], the link state information of a node includes not only its links to its neighbors, but to all the second hop neighbors as well. If on average, a node in the network has N neighbors, the links announced in the FSRL by a single node would be N*N (N neighbors, each neighbor also has N neighbors). As the fisheye scope of H-LANMAR is set to be 2, there are at least N*N nodes in a fisheye scope, the FSRL exchanged by the nodes within the fisheye scope would be N*N*N for a control time interval. In addition to the FSRL message, for the H-LANMAR, there are also LMU update messages propagated in the whole network. On the other hand, with the same network connectivity, in H-OLSR, each HELLO message would only exchange N links (N neighbors), and TC/HTC propagation is limited to the cluster/group area. If in a cluster with N*N nodes, there are N*N HELLO message exchanged. Therefore, compared to H-LANMAR, H-OLSR's routing overhead is much lower.

4.2.1.3 Packet Delivery Ratio

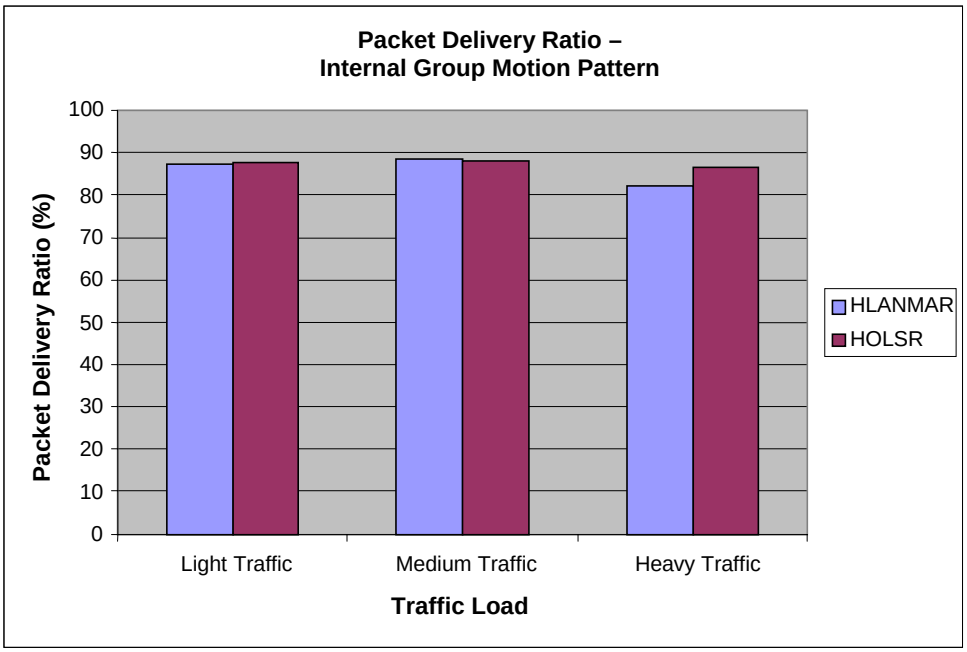

Figure 4.2.2 Packet Delivery Ratio Under Different Traffic Loads for Internal Group Motion

Packet Delivery Ratio: With a strict Internal Group Motion where there is no drifting node in the network, H-OLSR and H-LANMAR almost have the same packet delivery ratio. Because movement is restricted to a small area, the additional overhead caused by topology change is quite small. So even though H-LANMAR introduces heavy control overhead, its impact is not large enough to affect data packet delivery.

4.2.1.4 End-to-End Delay

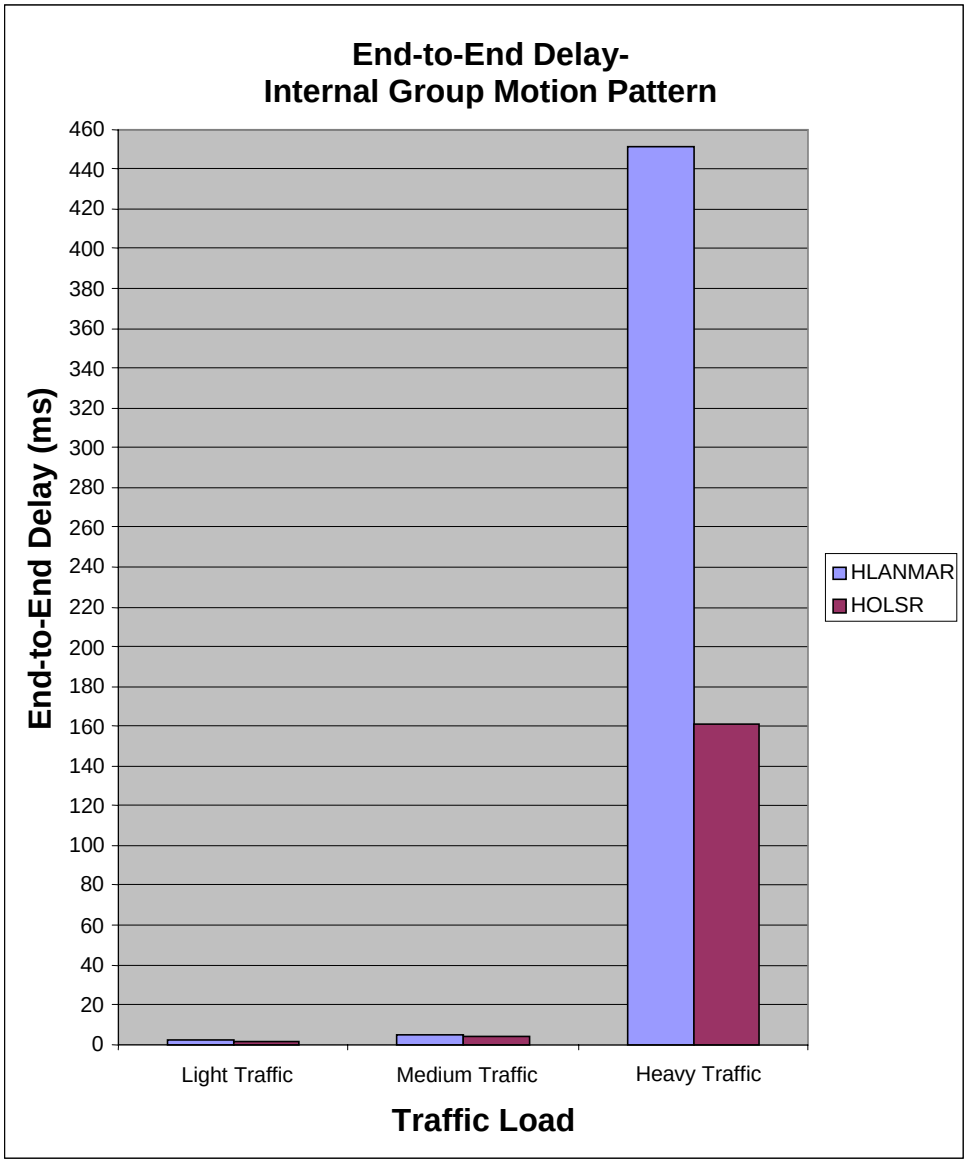

Figure 4.2.3 End-to-End Delay Under Different Traffic Loads for Internal Group Motion

End-to-End Delay: End-to-End delay is mainly determined by network traffic load, which includes both routing control traffic and data traffic. When nodes move strictly within their group area, the End-to-End delay of H-OLSR and H-LANMAR's data packets are almost the same under Light Traffic and Medium Traffic loads. However, under Heavy Traffic load, the End-to-End data delay of both H-OLSR and H-LANMAR increases, but the increase of H-LANMAR is much larger. Although the

control overhead of H-LANMAR is relatively light under the Internal Group Motion pattern compared to that under other motion patterns, it is still higher than that of H-OLSR. The impact of such high overhead on the End-to-End data packet delay may not be significant when the data traffic load is low, but is quite noticeable when there is heavy data traffic in the network.

4.2.2 The Internal Group Motion Pattern With Drifting Nodes

4.2.2.1 Movement Pattern Description

This movement pattern is a special case of the Internal Group Motion Pattern (section 4.2.1). In this movement pattern, the majority of the nodes move within their group area, while some nodes leave the group and move around the whole simulation area. Such scenario creates drifting nodes in the network. We introduce different percentages of drifting nodes to observe the impact on the performance of the routing protocol. In the experiments, the scenario with 20% of drifting nodes is denoted as HOLSR_20% with H-OLSR as routing protocol and HLANMAR_20% with H-LANMAR as routing protocol; similarly, the scenario with 40% of drifting nodes is denoted as HOLSR_40% and HLANMAR_40%. The parameters defined for this scenario are as follows:

Parameters	Values
Mobility model	A group stays in a fixed location Majority of nodes randomly move inside a group, others drift outside of the group (Random Waypoint mobility model with max speed of 10m/s, min speed of 0m/s, no pause time)
Distribution of nodes	10 nodes in each group 9 groups
Global simulation area	1200m * 1200 m
Local area of a group	200m*200m

Table 4.2.3 Parameters For The Internal Group Motion With Drifting Nodes Pattern

4.2.2.2 Normalized Routing Overhead

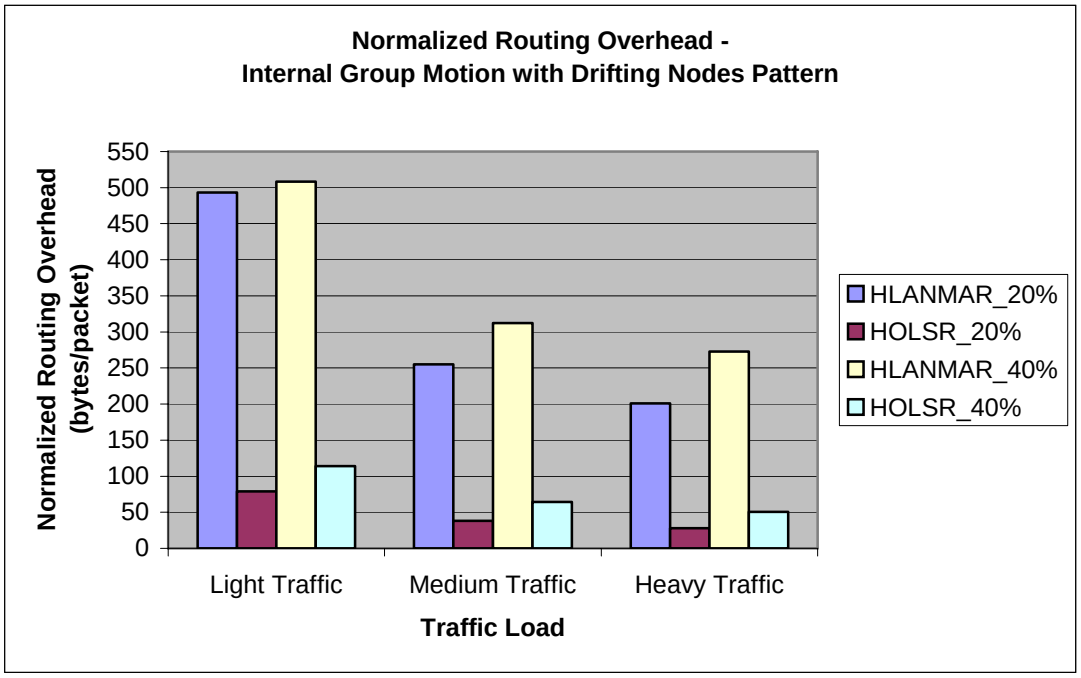

Figure 4.2.4 Normalized Routing Overhead Under Different Traffic Loads for Internal Group Motion With Drifting Nodes

Control Overhead: When there are drifting nodes in the network, H-LANMAR appends the drifting node information DFDV in the LMU message, and in doing so, further increases the control overhead. In order to build a shortest path from the landmark to a drifting node, each node on the shortest path needs to send a LMU message with an appended DFDV entry. If the drifting node is far away from the landmark, or if there is a large percentage of drifting nodes, the routing overhead caused by appended DFDV entry will increase further. Since H-LANDMAR's design was conceived on a predefined group concept, drifting nodes are not handled efficiently and cause a larger overhead than H-OLSR.

4.2.2.3 Packet Delivery Ratio

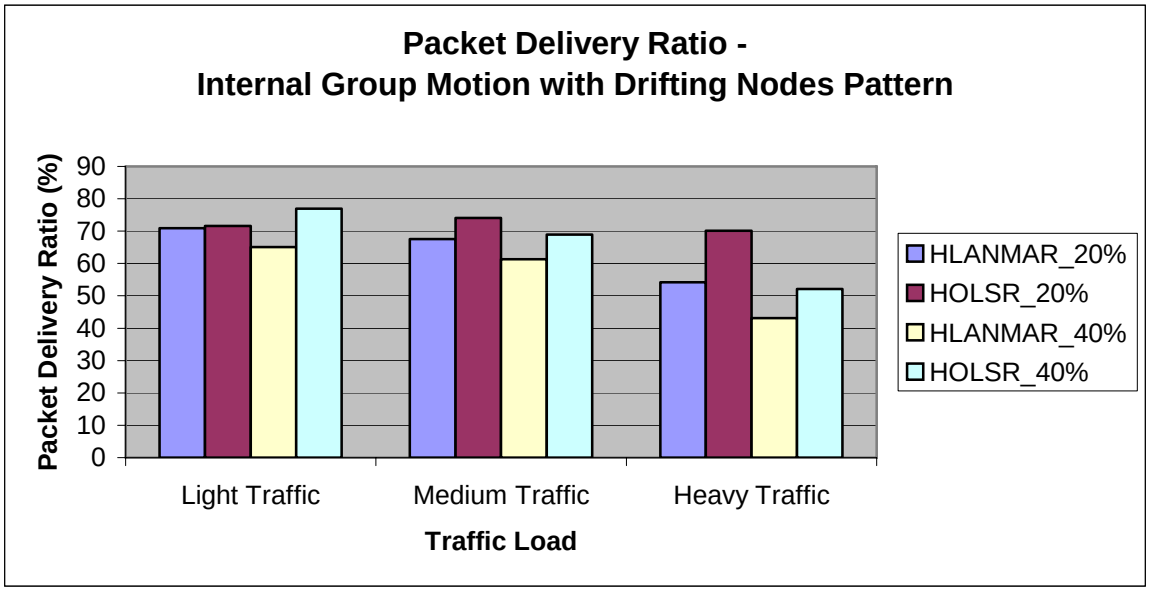

Figure 4.2.5 Packet Delivery Ratio Under Different Traffic Loads for Internal Group Motion With Drifting Nodes

Packet Delivery Ratio: When drifting nodes are introduced, packet delivery ratios of both H-OLSR and H-LANMAR are lower because nodes may lose connectivity at some point while drifting between groups. However, H-OLSR outperforms H-LANMAR in terms of packet delivery, as drifting nodes further increase traffic overhead of H-LANMAR. When a node moves into the scope of another logical group and becomes a drifting node to its logical group, an entry in the drifting distance vector is needed for routing to this node. As shown in Figure 3.1.4, a drifting node D1 will send a drifting distance vector to its landmark node L. If node P1 sends a packet to drifting node D1, the packet will be sent to landmark node L first. Then, landmark node L will send the packet to drifting node D1 according to the entry created by the drifting distance vector. In this case, a very long routing path is created when a node in the visiting network sends a packet to the drifting node, as packets are first routed to the landmark, then to the final destination, even when the destination node and the landmark are in different areas of the network. This H-LANMAR strategy results in a longer path to the drifting nodes, which increases the probability of data packets collision/dropping along the path. H-OLSR, on the contrary, does not restrict node movement pattern. The H-OLSR clusters are automatically formed, so nodes can join/leave a specific group freely. Because of H-LANMAR's request for predefined groups, H-OLSR handles the problem of drifting nodes much better.

4.2.2.4 End-to-End Delay

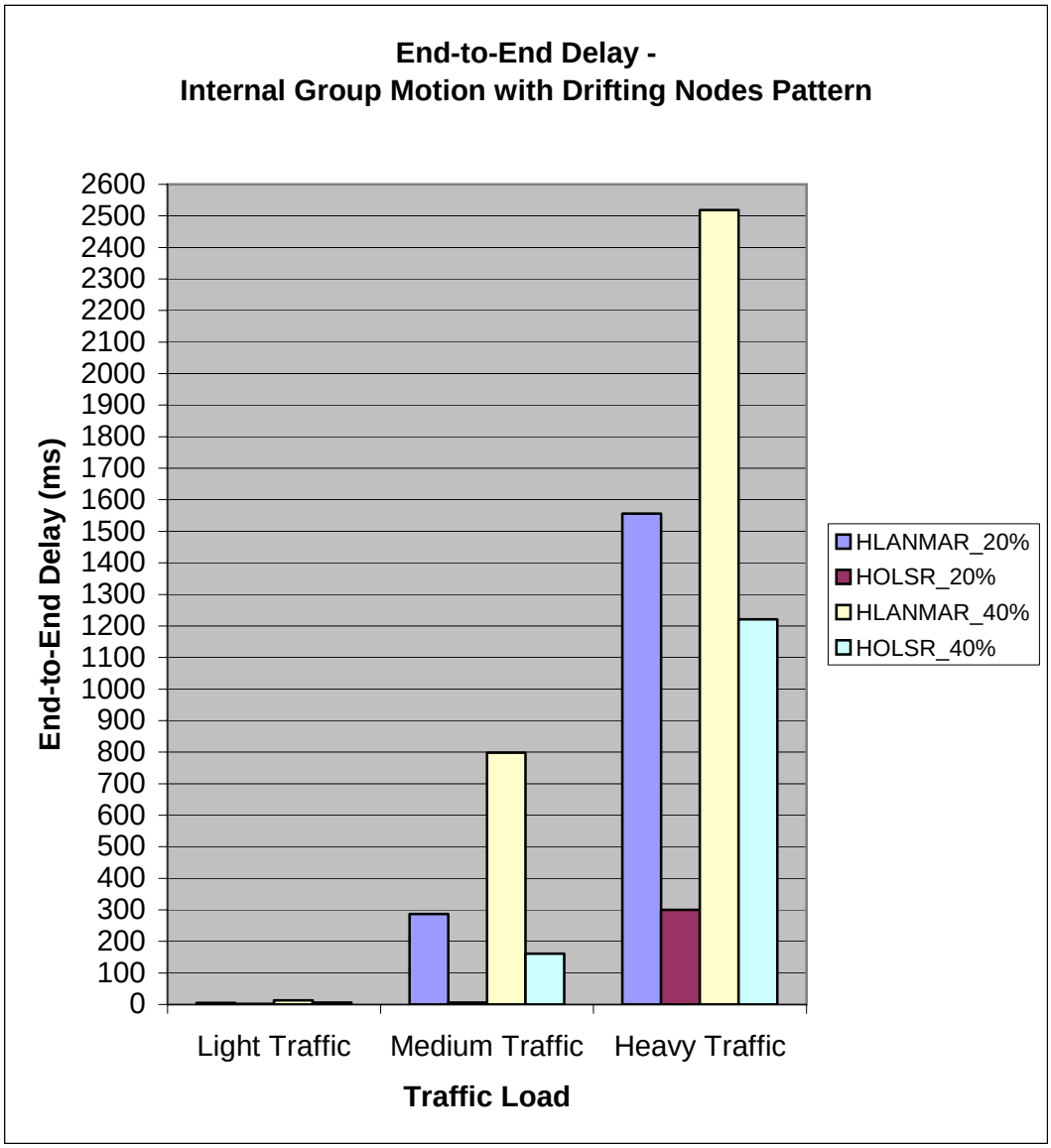

Figure 4.2.6 End-to-End Delay Under Different Traffic Loads for Internal Group Motion With Drifting Nodes

End-to-End Delay: When drifting nodes are introduced into the internal group motion pattern, the end-to-end delay of both H-OLSR and H-LANMAR is larger than that without drifting nodes because frequently changing topology with drifting nodes triggers more control messages that competes with data packets for channel access. However, H-OLSR still delivers data packets faster than H-LANMAR. The difference comes from two aspects: 1) H-LANMAR's high control overhead when dealing with

drifting nodes causes network congestion, 2) the path to the drifting nodes may not be the optimal/shortest path, as data to the drifting nodes is first sent to the landmark. If the landmark and the drifting node are located in different areas, the data may be delivered along a longer and indirect path.

4.2.3 The Group Moving Pattern

4.2.3.1 Movement Pattern Description

The Reference Point Group Mobility (RPGM) model [1] is used for modeling the Group Mobility pattern. In this movement model, nodes in the same group always move together. Each group has a "group leader", who determines the velocity and direction of the movement of the group. The group leader moves based on the Random Waypoint mobility model [10]. Nodes can communicate within a group or between groups. We define the parameters in this mobility model as follows:

Parameters	Values
Mobility Model	RPGM
Distribution of Nodes	10 nodes in each group 9 groups
Global simulation area	1200m * 1200 m
Maximum Distance to Group Center	100 m

Table 4.2.4 Parameters For The Group Moving Pattern

4.2.3.2 Normalized Routing Overhead

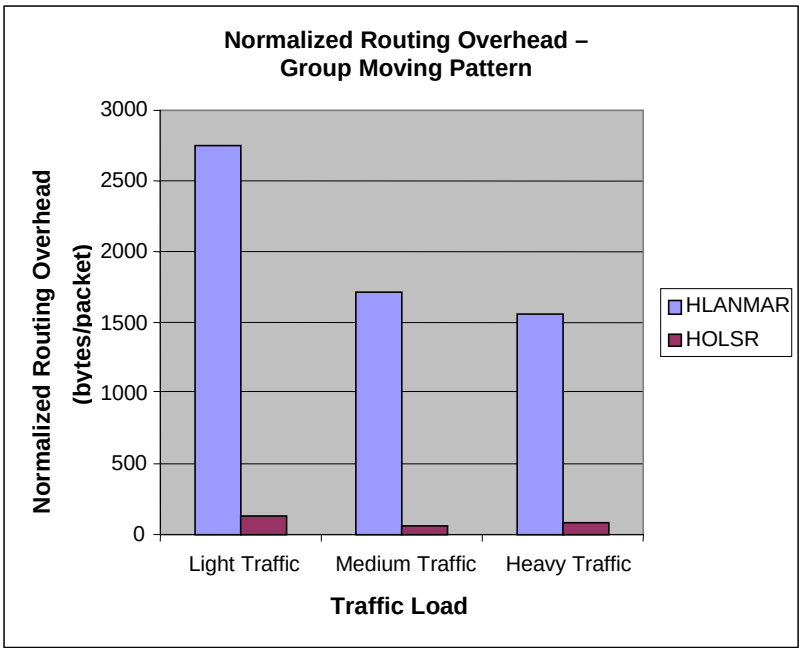

Figure 4.2.7 Normalized Routing Overhead Under Group Moving

Control Overhead: Under all traffic loads in the Group Mobility pattern, H-OLSR's control overhead is much lower than that of the H-LANMAR, for the same reasons explained in previous sections. With the same movement speed and same traffic load, H-LANMAR's control overhead under Group Moving pattern is much higher than that under Internal Group Motion pattern (***Figure 4.2.1***). Group Moving pattern introduces more topology change than Internal Group Motion pattern, which makes the proactive routing protocols send more control traffic to update the topology information. However,these figures also show that H-OLSR's routing overhead increase in Group Moving pattern is not as drastic as that of H-LANMAR. This is because in H-OLSR, the propagation of topology control messages is limited to the local area, which prevents these messages from being flooded into the entire network. In other words, H-OLSR handles topology change more efficiently than H-LANMAR under the scenario with the Group Moving pattern.

4.2.3.3 Packet Delivery Ratio

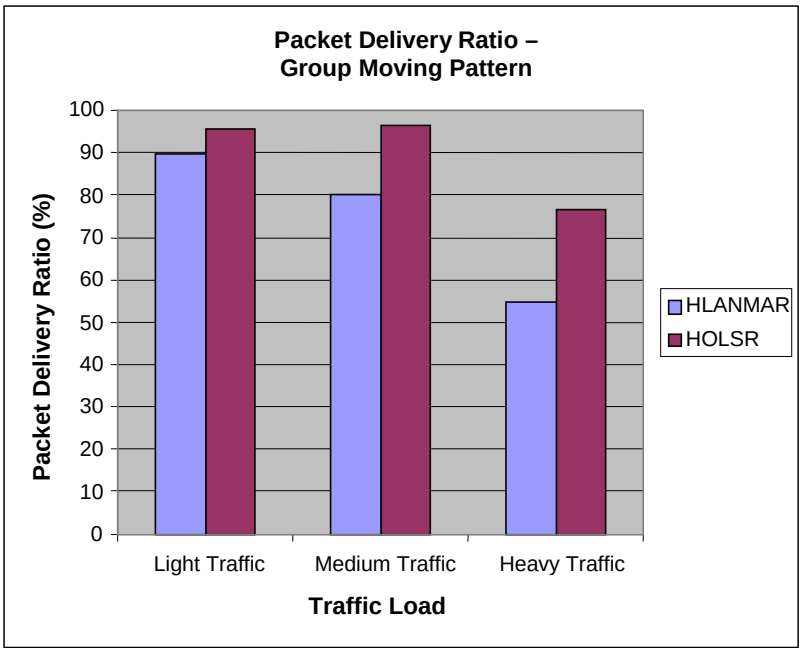

Figure 4.2.8 Packet Delivery Ratio Under Group Moving

Packet Delivery Ratio: With the increase of topology change in Group Moving pattern, the high routing overhead that H-LANMAR introduces begins to show its detrimental effect. In all of the three different network traffic loads under Group Moving pattern, H-OLSR has a higher data packet delivery ratio than H-LANMAR, although H-LANMAR claims to be suitable for group movement scenarios From the experimental results, we can observe that even though the H-LANMAR is designed for group movement, the non-optimal in-scoped routing can still prevent it from achieving good performance.

4.2.3.4 End-to-End Delay

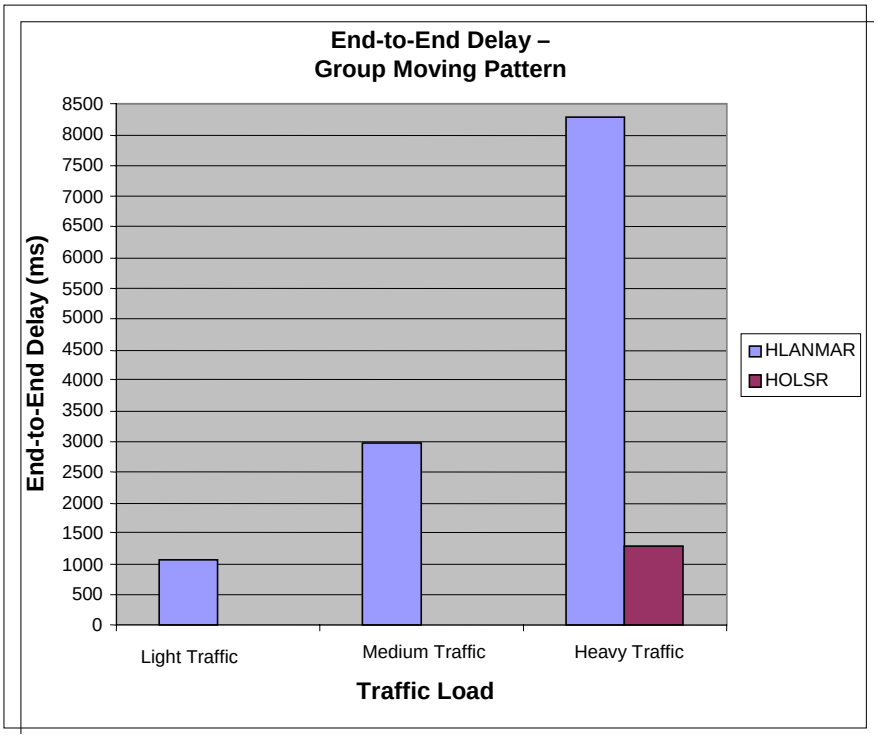

Figure 4.2.9 End-to-End Delay Under Group Moving

End-to-End Delay: Again, the high routing overhead makes H-LANMAR deliver data packets slower than H-OLSR in each of the three network traffic loads under Group Moving pattern. Especially with the heavy network traffic load, H-LANMAR's data packet End-to-End delay is extremely large compare to that of H-OLSR.

4.2.4 The Group Merging Pattern

4.2.4.1 Movement Pattern Description

In this movement pattern, all groups merge together. Any mobile node can move in the whole simulation area. The Random Waypoint mobility model [10] was used to generate the movement of a node. Any mobile node can communicate with any other mobile node. Using this model, there is no hierarchical address structure in the MANET. Any routing mechanism based on the group concept will be challenged. However, in a military scenario where an emergency action is required, this is not an unusual situation. This type of movement pattern is necessary to consider when dealing with military tactical MANETs. The parameters defined for this pattern are described in the following table.

Parameters	Values
Mobility model	All nodes randomly move in the global simulation area (Random Waypoint mobility model)
Distribution of nodes	10 nodes in each group 9 groups All 9 groups merge together
Global simulation area	1200m * 1200 m

Table 4.2.5: Parameters For The Group Merging Pattern

4.2.4.2 Normalized Routing Overhead

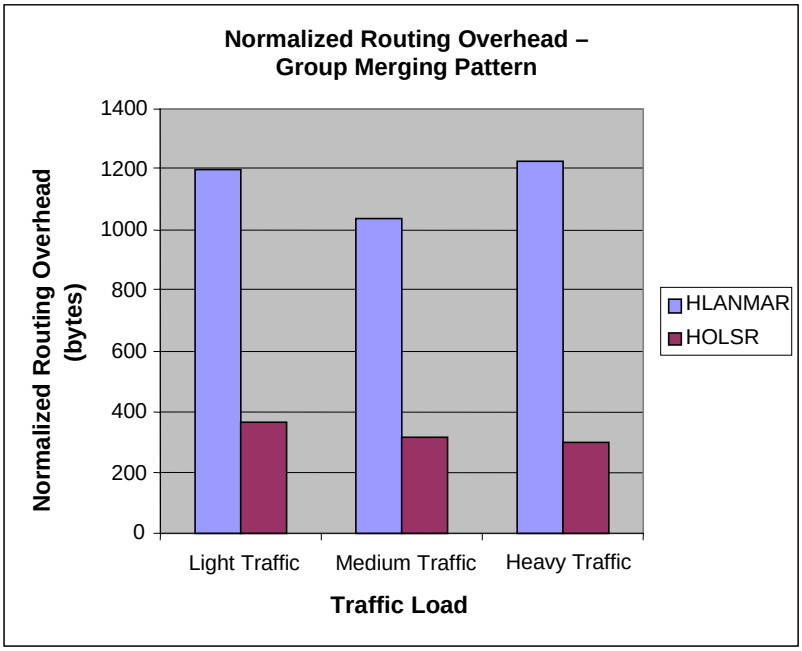

Figure 4.2.10 Normalized Routing Overhead Under Group Merging

Control Overhead: Among all the four movement patterns studied in this report, the Group Merging movement pattern introduces the most drastic topology changes as all nodes move freely in the global simulation area regardless of their original group position. So it is reasonable that with the same movement speed and same traffic load, H-OLSR's control overhead under Group Merging pattern is much higher than that with Group Moving Pattern (***Figure 4.2.7***). However, Figure 4.2.7 and Figure 4.2.10

show that the H-LANMAR's control overhead is lower under the Group Merging pattern than under the Group Moving pattern. This "abnormal" situation comes from the lower node density under Group Merging pattern, which results in less routing message being propagated by H-LANMAR. Under Group Merging pattern, all nodes randomly and evenly distribute in the 1200m*1200m area no matter which group they belong to. Node density is lower comparing to Group Moving pattern where a group of nodes always bind together. Routing message size of H-LANMAR increases as node density increases because the routing message size is proportional to N*N*N for each interval, if each node has N neighbors on average. Meanwhile, similar to previous movement patterns, the H-OLSR's routing overhead is much less than that of H-LANMAR for all three scenarios studied under the current movement pattern.

4.2.4.3 Packet Delivery Ratio

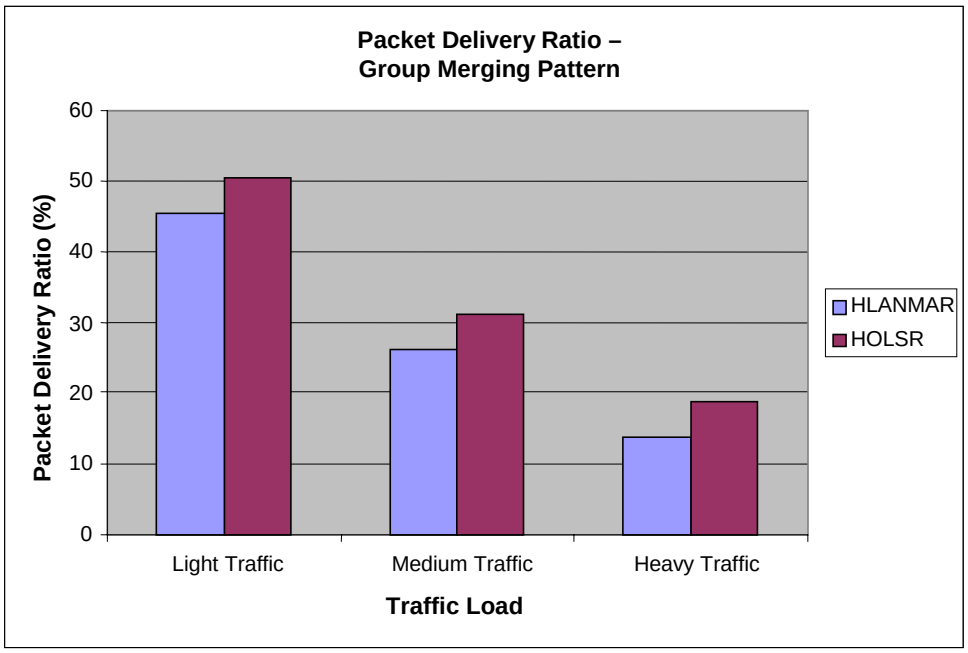

Figure 4.2.11 Packet Delivery Ratio Under Group Merging

Packet Delivery Ratio: With the drastic topology changes and the high routing overhead from both routing protocols, the performance of the network degrades under this movement pattern. So here, the packet delivery ratio for both H-OLSR and H-LANMAR under all three traffic loads is much lower than the matching scenarios under Group Moving pattern. Again, similar to the previous movement patterns, the packet delivery ratio of H-OLSR is higher than that of H-LANMAR, because of H-

OLSR's relatively lower control messages overhead (which causes less network congestion).

4.2.4.4 End-to-End Delay

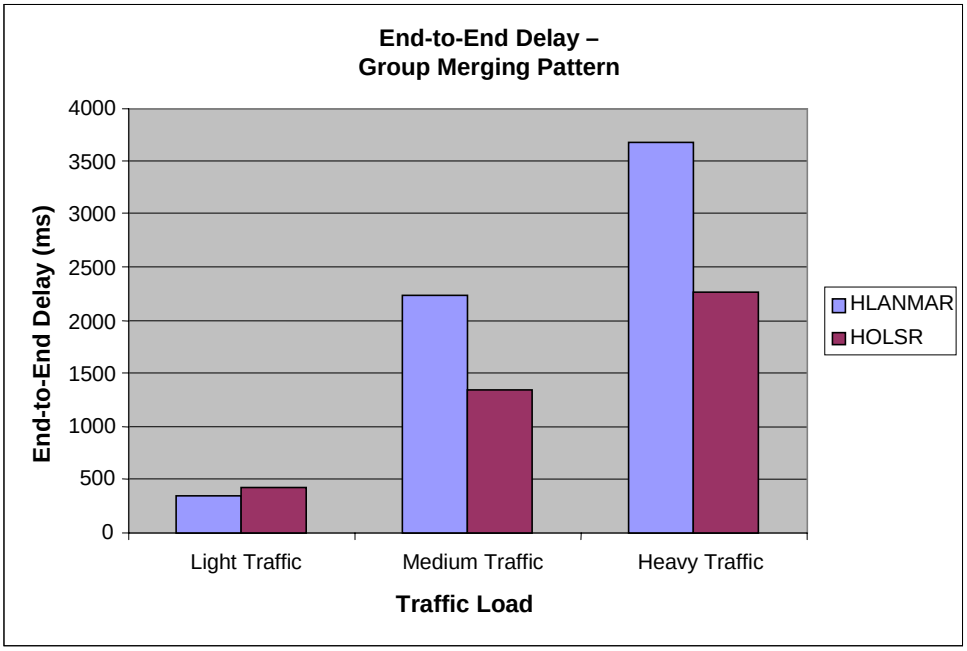

Figure 4.2.12 End-to-End Delay Under Group Merging

End-to-End Delay: The high routing overhead introduced by the continuous topology changes makes the End-to-End delay of both H-OLSR and H-LANMAR very large. Under the Group Merging pattern, H-OLSR delivers data packets faster than H-LANMAR under medium and heavy traffic load, but under Light Traffic Load, the End-to-End delay of H-OLSR is slightly higher than H-LANMAR. The explanation to this observation lies in the way H-LANMAR and H-OLSR work. For H-LANMAR, if logical groups merge together, the nodes in the merging groups will include each other in their routing table instead of routing through the landmarks. Packets will be delivered using the shortest path. H-OLSR still routes packets through cluster heads if two nodes belong to different clusters. The path may not be the shortest one, but is the one with the highest capacity link. Under light traffic load, shortest path is the key for short End-to-End delay. Thus, H-LANMAR has better performance. However, under medium or heavy traffic load, the queue waiting time of low capacity links becomes the dominant component of End-to-End delay. Compared to H-LANMAR which delivers packets through low capacity links, H-OLSR delivers packets over high capacity links through cluster heads and has less waiting time, thus the End-to-End delay is smaller than with H-LANMAR.

4.2.5 Conclusion

From the simulation results, we can see that the most suitable scenario for the H-LANMAR is when nodes are always moving in groups and when the groups always have a stable landmark without any drifting nodes. When nodes move strictly within their group area and the network traffic load is not too heavy, H-OLSR and H-LANMAR perform equally well in terms of data packet delivery ratio and end-to-end delay. Therefore under such a scenario, both H-OLSR and H-LANMAR are suitable. However, when the network topology changes frequently or network traffic load is high, H-OLSR outperforms H-LANMAR in terms of the packet delivery ratio and the end-to-end delay. H-LANMAR was designed to support group mobility. If two logical groups mix together, the nodes in the two groups will include each other in their routing table instead of routing through the landmark node. In this case, the algorithm does not exploit the advantage of small routing table size and lower bandwidth overhead. The landmark election and LMDV propagation will still be used, causing additional overhead. The heavy routing overhead in H-LANMAR and the way it handles the drifting nodes prevent H-LANMAR from showing good performance.

However, there may be ways to improve H-LANMAR to reduce its overhead such that it may provide better performance. Such improvement may include optimizing the radius of the fisheye scope, or to employ a different in-scope routing scheme. Further studies would be required to analyze how the H-LANMAR in-scope routing scheme could be optimized.

5. Discussion

The objective of this report was to investigate two different hierarchical routing schemes to facilitate the use and the design of a mobile ad hoc network for tactical operations. Our goal was to set a direction for the selection of a routing scheme for a typical tactical MANET. Two proactive hierarchical routing protocols, namely H-OLSR and H-LANMAR where described and the benefits and issues of each were analyzed. Based on available implementations, simulation results were presented to demonstrate the performance of the two routing protocols under different group mobility patterns. The applicability of the two routing protocols for a military tactical scenario was assessed based on the simulation results.

Based on our test results, we demonstrated that both H-LANMAR and H-OLSR could adapt to topology changes during a tactical mission but with different performance results. H-LANMAR was designed primarily to handle a group movement pattern where each group has an associated landmark and where data are transmitted between the groups via the corresponding landmarks. We observed that the overhead caused by the out-scoped routing was light but that the in-scope routing mechanism in the available implementation introduced a significant amount of overhead and thus reduced the overall performance of H-LANMAR. The FSR in-scope routing approach was restricted in that it did not show progressively less detailed routing information as the distance increased. The topology information of all nodes inside scope was propagated every interval. All the nodes outside of the scope became drifting nodes causing a high exchange of messages. Improvements to the implementation are required to support graded update rates in multiple scopes in order to reduce the high control overhead. One way of reducing the overhead incurred with H-LANMAR is to use another protocol to support the in-scope routing. An advantage of H-LANMAR is its flexibility to adapt to any in-scoped routing protocol. As a consequence OLSR could be integrated as the in-scoped routing protocol, which would result in a better performance because the control overhead would be reduced. This aspect can be further investigated in future work.

H-OLSR is derived from OLSR and introduces the concept of cluster and cluster heads. The cluster is formed in a dynamically and timely way by adding light control overhead in low capacity link. The hierarchical extension used in H-OLSR highly depends on the original OLSR internal mechanisms. Therefore, it is not easy to integrate the H-OLSR hierarchical extension into other flat routing protocols.

H-LANMAR was designed for pure group mobility without inter-group movement activities. The routing to a drifting node in H-LANMAR needs special treatment since H-LANMAR relies on a hierarchical addressing scheme or predefined group ID. If many nodes move between groups, a large number of drifting nodes will cause high overhead and non-optimized routes. Group merging requires a mechanism

to distribute a temporary group ID or combine the two group IDs to form a temporary group ID in order to keep the advantage of small routing table size and lower bandwidth. Group partitioning requires the tuning of a parameter that reflects the new scope size if the landmark election is to work properly.

H-OLSR is flexible and can support group mobility, movement within groups, and group merge because of the way the clusters are formed and the routing does not rely on a logical hierarchical addressing scheme. Unlike most routing protocols for large scale MANET (such as H-LANMAR) restricted in hierarchical addressing structures or predefined group ID, the logical hierarchical addressing scheme or predefined group ID is not necessary for H-OLSR.

In a military tactical scenario, if cluster heads or backbone nodes are destroyed or unavailable, both routing protocols can revert to a flat protocol namely OLSR and LANMAR and continue to work normally without a failure point.

The simulation results under different group movement patterns show that H-OLSR introduces lower routing overhead than H-LANMAR, and has better performance in terms of packet delivery ratio and end-to-end delay. The H-LANMAR is further degraded when drifting nodes are introduced. Our assertion at this point is that H-OLSR is a better candidate for supporting various mobility patterns as its clustering mechanism is very flexible and does not require a logical hierarchical addressing scheme and can therefore adapt easily to group merges. However, if an addressing scheme is required, one can be employed as it might be the case in some specific scenarios where a network exhibits group mobility where the participants all move together.

6. References

[1] L. Genik, M. Slamanian, P. Mason, H.A. Schotanus, C.A.A. Verkoelen and E. Hansson, “Mobile Ad Hoc Network Security from a Military Perspective”, Technical Report, DRDC Ottawa, TR 2004-252, Dec. 2004.
[2] Z. Hass, M. Pearlman, P. Samar, “The Zone Routing Protocol (ZRP) for Ad Hoc Networks”, draft-ietf-manet-zone-zrp-04.txt, Jul. 2002.
[3] Z. Hass, M. Pearlman, “The Performance of Query Control Schemes for the Zone Routing Protocol”, IEEE/ACM Transactions on Networking, Vol. 9, No. 4, Aug. 2001.
[4] G. Pei, M. Gerla and X. Hong, “LANMAR: Landmark Routing for Large Scale Wireless Ad Hoc Networks with Group Mobility”, Proceedings of IEEE/ACM MobiHOC 2000, Boston, MA, Aug. 2000.
[5] G. Pei, M. Gerla, and T.-W. Chen, “Fisheye State Routing: A Routing Scheme for Ad Hoc Wireless Networks”, Proceedings of ICC 2000, New Orleans, LA, Jun. 2000.
[6] Ying Ge, Louise Lamont, Luis Villasenor, "Hierarchical OLSR -- A Scalable Proactive Routing Protocol for Heterogeneous Ad Hoc Networks", WiMob 2005 Wireless and Mobile Computing, Montreal, Canada, Aug. 22-24, 2005.
[7] Luis Villasenor-Gonzalez, Ying Ge, Louise Lamont, "H-OLSR: A Hierarchical Proactive Routing Mechanism for Mobile Ad Hoc Networks", IEEE Communications Magazine, Vol 43, No. 7,Jul. 2005.
[8] K.Xu and M.Gerla, “A Heterogeneous Routing protocol Based on a New Stable Clustering Scheme”, IEEE Military Communications Conference (MILCOM), Anaheim, CA, Oct. 2002.
[9] C.E.Perkins and E.M.Royer, “Ad-Hoc On-Demand Distance Vector Routing”, IEEE WMCSA 1999, New Orleans, LA, Feb. 1999.
[10] Deepanshu Shukla, “Mobility Models in Ad Hoc Networks”, Master’s thesis, KReSIT-ITT Bombay, Nov. 2001.
[11] David B. Johnson, “Safari: A Self-Organizing, Hierarchical Architecture for Scalable Ad Hoc Networking”, http://research.microsoft.com/india/events/wins2006/presentations/David%20Johnson_Plenary2_Apr7.ppt
[12] David B. Johnson, David A. Maltz, and Josh Broch. “DSR: The Dynamic Source Routing Protocol for Multi-Hop Wireless Ad Hoc Networks. In Ad Hoc Networking,” edited by Charles E. Perkins, Chapter 5, pp. 139-172, Addison-Wesley, 2001.
[13] T. Clausen, P. Jacquet, “ Optimized Link State Routing Protocol (OLSR)”, IETF MANET RFC3626, Oct. 2003.
[14] V. Devarapalli, R. Wakikawa, A. Petrescu, P. Thubert, IETF RFC 3963 “Network Mobility (NEMO) Basic Support Protocol (RFC 3963)”, Jan. 2005.
[15] Joseph Macker, Jeff Weston, Louise Lamont, Thierry Plesse, Wolfgang Fritsche, Ivano Guardini, Boris Kock, Knut Ovsthus, Harald Bongartz, Michael Clark, Interoperable Networks for Secure Communications, Task3, Mobile Networking Technology Assessment and Considerations Report, June 2005.

[16] Microsoft Corporation, “Understanding Mobile IPv6”, April 2004.

Appendix A. Network Edge Mobility

A.1 Introduction to NEMO

Edge mobility arises when a portion of the network changes its point of attachment to the network. When a node or a group of nodes moves, it can be unplugged from the previous connector, and plugged into a new point of attachment. However, ongoing data transfers would be lost and session would be broken during the migration if no specific services handle mobility. The protocol stack must be upgraded with the ability to cross networks in the midst of data transfers, without breaking the communication session and with minimum transmission delays and signaling overhead. In an IPv6 network, this is referred to as Mobile IPv6 for supporting node mobility and as Network Mobility (NEMO) [14][15] for supporting network mobility. NEMO is essentially an extension to Mobile IPv6. In order to understand NEMO, a brief introduction to Mobile IPv6 will first be presented.

A.1.1 Node Mobility (Mobile IPv6)

A node in a network is defined with an IP address which serves two purposes: a unique identifier for a communication endpoint; an indicator of location for hierarchical routing structure. When a node moves, it needs to change to a new address which reflects its current location. However, this implies that the node is not reachable with its previous identifier. In order to keep a node's identifier as well as keep the connectivity during migration, Mobile IPv6 is proposed. Mobile IPv6 is designed to allow mobile devices to move from one network to another while maintaining their permanent IP address. ***Figure A.1*** shows the components of Mobile IPv6[16].

- **Mobile Node (MN):** An IPv6 node that can change links, and therefore addresses, and maintain reachability using its home address.
- **Home Link:** The link from which the mobile node originates.
- **Home Address:** An address assigned to the mobile node when it is attached to the home link and through which the mobile node is always reachable, regardless of its location on an IPv6 network.
- **Home Agent (HA):** An entity on the home link that maintains registrations of the mobile nodes that are away from home and are at their current addresses. The home agent forwards traffic to mobile nodes while they are away from the home link.
- **Foreign Link:** A link that is not the mobile node's home link.
- **Care-of Address (COA):** An address associated with current location and used by a mobile node while it is attached to a foreign link. The association of a home address with a care-of address for a mobile node is known as a *binding.*

- **Correspondent Node (CN):** An IPv6 node that communicates with a mobile node.

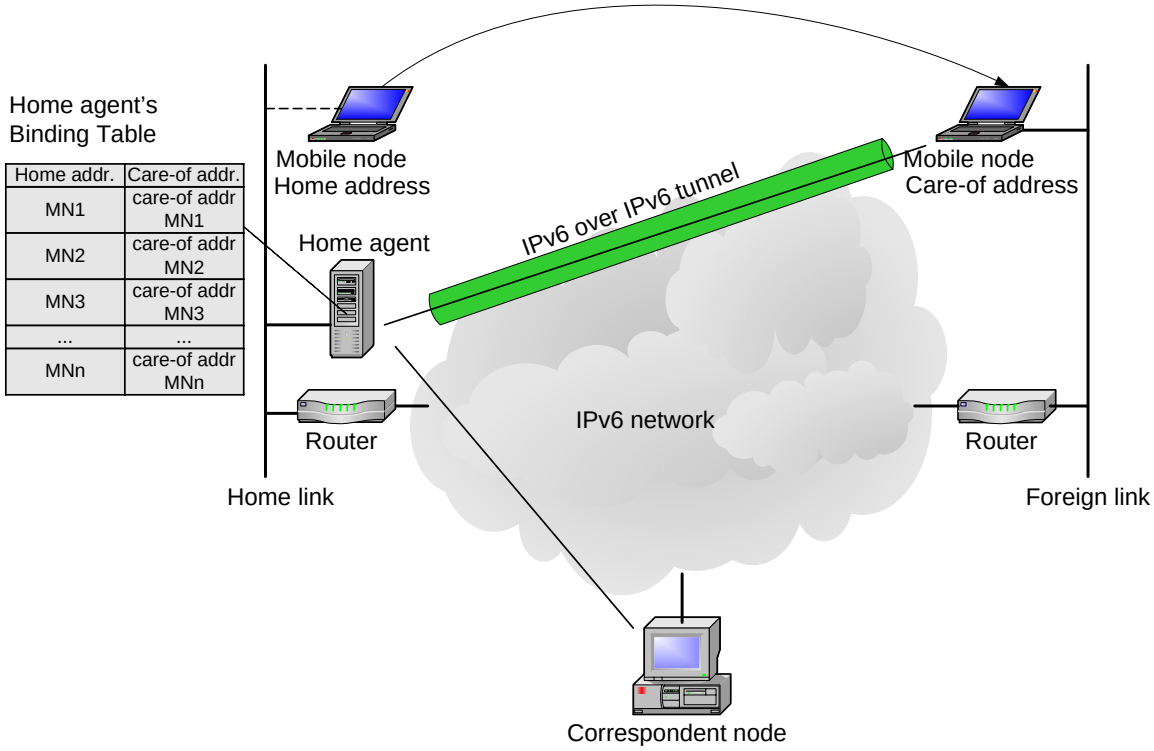

Figure A. 1 A Mobile Node Moves in a Mobile Network

When a node moves to a foreign link, it acquires a care-of address which is assocated with its current location. The mobile node sends its care-of address in a binding update message to its home agent. The home agent records the assocation of the mobile node's home address with its current care-of address.

- A correspondent node sends data packets to a mobile node by using the mobile node's home address. Data packets arrive the mobile node's home network and are intercepted by the home agent. The home agent encapsulates data packets with an outer IPv6 header and tunnels data packets to the mobile node's current location using IPv6-over-IPv6 tunneling. In the outer IPv6 header, the mobile node's care-of address is the destination address and the home agent's address is the source address. At the other end of the tunnel, data packets are decapsulated to remove the added IP header, and delivered to normal TCP/IP stack inside the mobile node.

- When a mobile node sends data packets to a correspondent node, the data packets are first sent to the home agent using IPv6-over-IPv6 tunneling. Inside the IPv6 header, the correspondent node's address is the destination and the mobile node's home address is the source. In the outer IPv6 header, the home agent address is the destination and the care-of address is the source. At the other end of tunnel, the home agent removes the outer IPv6 header of the data packets and forwards them to the correspondent node.

The home agent works as an anchor point for mobile nodes at their home network. However, the data transmission path is not optimized. If a correspondent node is Mobile IPv6 capable, data packets can be sent to the correspondent node directly without going through the home agent. It is referred as the route optimization in Mobile IPv6. Since security problems still exist for route optimization, we will not further discuss route optimization here.

A.1.2 Network Mobility

Network Mobility (NEMO) is essentially an extension to Mobile IPv6. NEMO is designed to apply to the entire network in motion, rather than just individual nodes in motion. When a network moves, NEMO keeps every node in the network reachable with their communication partners.

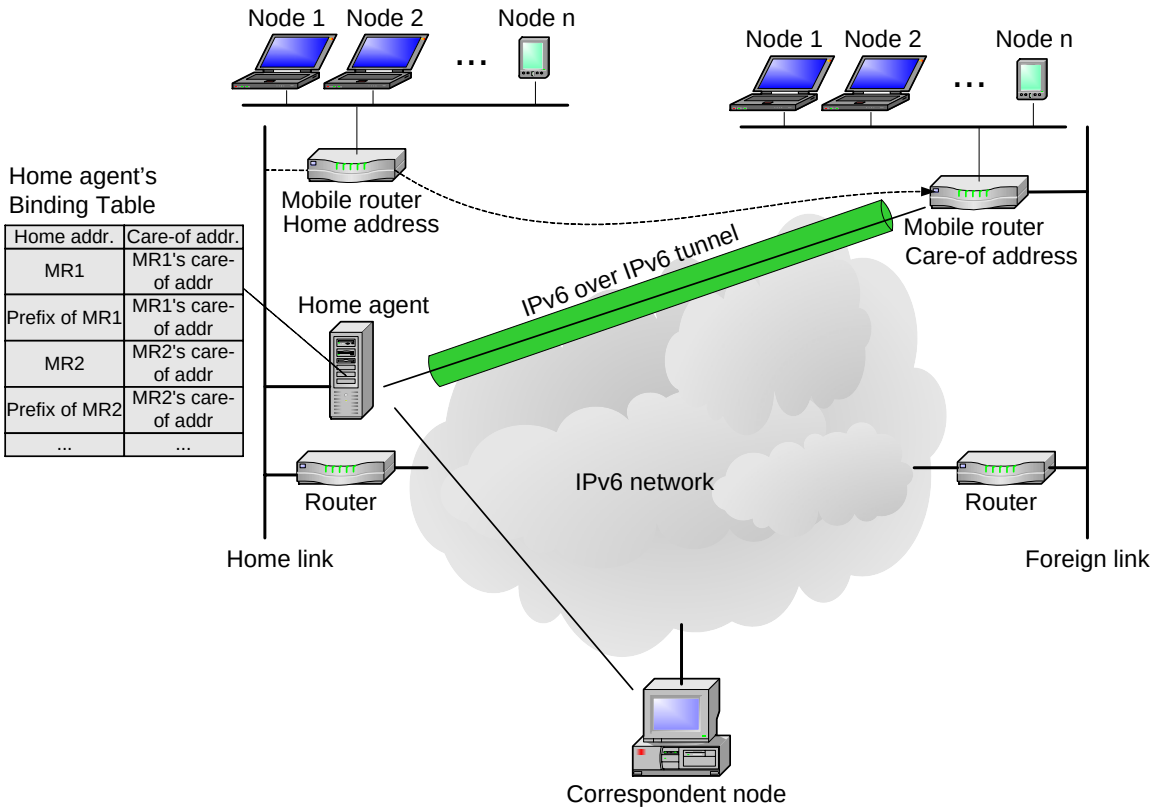

Figure A. 2 A Mobile Network Moves in a Mobile Network

Figure A. 1 and ***Figure A. 2*** show the difference between node mobility and network mobility. Instead of a mobile node moving, the entire network behind a mobile router moves. The basic support protocol is run between a new entity called the mobile router and the home agent.

- Mobile Router (MR): a router capable of changing its point of attachment to IPv6 network, moving from one link to another link, which acts as a gateway between an entire mobile network and the rest of IPv6 network. The MR provides routing services and reachability to the nodes attached to it within the mobile network.

The mobility of the MR and the network as a whole is transparent for the nodes within the mobile network. In the case of Mobile IPv6, an alternative solution for ordinary client machines is to simply obtain a new address and restart any existing sessions. However, such an alternative is not recommended for mobile networks, because it requires every node within the mobile network to obtain a new address in a local prefix or the mobile router to inject specific host and/or network routes for the

mobile network into the WAN at its point of attachment. Neither of these options is particularly scalable for large numbers of mobile networks.

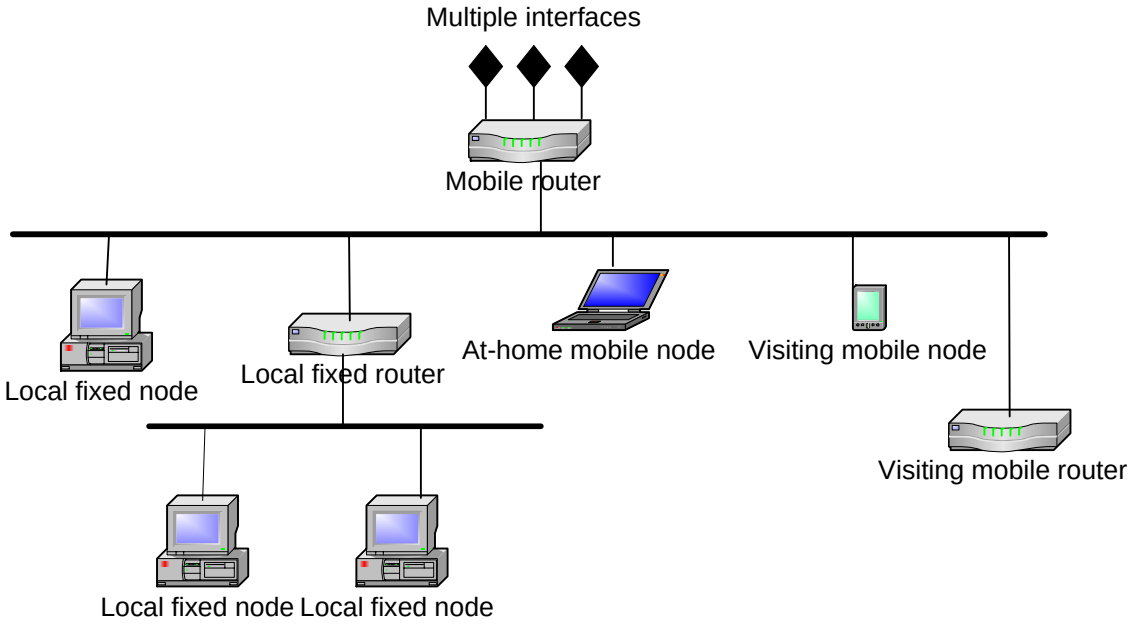

Figure A. 3 A NEMO Mobile Network

The mobile network can contain numerous local fixed nodes (LFN) and local fixed routers (LFR), as shown in ***Figure A. 3***, which are permanently attached to the mobile network. The mobile network can be the home network for Mobile IPv6 mobile nodes, and can also support visiting mobile nodes and/or the mobile routers attaching to it.

A.2 NEMO Support

In order to support the entire network mobility, a mobile router not only acts as a normal router but also has new mobility mechanism embedded. The home agent needs to be extended to support network mobility.

When a network behind a mobile router moves away from the home link and attaches to a new access router, the mobile router acquires a care-of address from the visited link. The mobile router will send a binding update to its home agent to indicate to the home agent that a node is functioning as a mobile router instead of a standard mobile node. A new flag (R) is set in the binding update. In the binding update, the mobile router informs the home agent that not only its home address but also the mobile network prefixes should be binding to its current care-of address. This indicates to the home agent that data packets destined to the mobile router as well as

any nodes in the mobile network should be forwarded to the mobile node's care-of address. The home agent will acknowledge the binding update by sending a binding acknowledgement to the mobile router. A positive acknowledgement with the mobile router flag (R) set means that the home agent has set up forwarding for the mobile network. Once the binding process finishes, a bidirectional tunnel is established between the home agent and the mobile router. The tunnel end points are the home agent's address and the mobile router's care-of address. The mobile router functions as a standard mobile node for sessions addressing the mobile router at its home address.

All packets originating from, or destined for, nodes in the mobile network are sent over a bidirectional tunnel between the mobile router and the home agent, similar to the Mobile IPv6 bidirectional tunneling mode.

- When a data packet originating from a node in the mobile network reaches the mobile router, the mobile router encapsulates the data packet and sends it to the home agent (reverse-tunneling). In the outer IPv6 header, the destination is the home agent's address; the source address is the mobile router's care-of address. In the inner IPv6 header, the destination is the correspondent node's address; the source address is the node's address. On the other end of the tunnel, upon the reception of the data packet, the home agent decapsulates it and forwards the packet to the correspondent node.
- Vice versa, when the home agent receives a data packet whose destination belongs to the set of mobile prefixes served by a mobile router, the home agent encapsulates the data packet with the mobile router's care-of address as the destination address and the home agent's address as the source address. The mobile router, upon the reception of the data packet, decapsulates and forwards it through the interface towards which the prefix is known to be reachable.

The binding process and data packet transmission scheme in NEMO ensure complete transparency of the network mobility to the nodes in the mobile network. Fixed nodes attached to the mobile network do not need mobility support. Visiting mobile nodes that attach to the mobile network treat the mobile network as a normal IPv6 access network and acquire care-of addresses based on the mobile router's home prefix. A visiting mobile node runs the normal Mobile IPv6 protocol and will send a binding update message to the mobile node's home agent to bind the acquired care-of address with the mobile node's home address. This binding update message is encapsulated by the mobile router and sent to the home agent of the mobile router. The message is decapsulated by the mobile router's home agent and is forwarded to the mobile node's home agent. All packets destined to the visiting mobile node will be first forwarded by the mobile node's home agent and then the mobile router's home agent. Finally they reach the mobile router and the visiting mobile node. This is called nested NEMO.

A.3 NEMO Benefits

NEMO extends the benefits of Mobile IPv6 to apply to entire networks in motion, rather than individual nodes. This extension results in a decrease in required protocol signaling traffic. The mobility is transparent to other nodes in the mobile network except the mobile router. Nodes in the mobile network do not need to be modified for mobility support.

A.4 NEMO Issues

While the NEMO basic support mode has been specified, work on the extended support mode addressing route optimization is still ongoing within the IETF. Therefore, the idea of nested NEMOs (one Mobile Router connecting to another Mobile Router's mobile network) currently results in additional encapsulated tunnels between the mobile router and the home agent. There are several possible methods for improving this, but they are not very well defined in the specification currently. Thus, any solution based on NEMOs at this time will possibly need to be changed at a later date to conform to more mature specifications.

The basic benefit of NEMO is the support of macro-mobility. However, it is not an appropriate protocol for managing significant amounts of local mobility.

A.5 Observation of NEMO Applicability

A.5.1 General NEMO Examples

An example of how NEMO technology can be conveniently exploited in an operational environment is presented in ***Figure A. 4***[15]. The example shows a military vehicle equipped with an on-board LAN, which may include several PCs and one or more Wireless Access Points (APs) for local Wireless LAN (WLAN) coverage. The WAN connectivity for this moving network is provided by a mobile router with multiple WAN interfaces (HF/VHF, satellite, WLAN, Ethernet, etc.). The NEMO protocol, which is implemented on the mobile router and on the Mobile IPv6 home agent located in the headquarters, gives the on-board LAN uninterrupted WAN connectivity independent of the radio access being used by the mobile router to plug into the tactical IPv6 backbone. The mobile router is free to select at any time the most convenient access technology, based on coverage conditions and vehicle velocity.

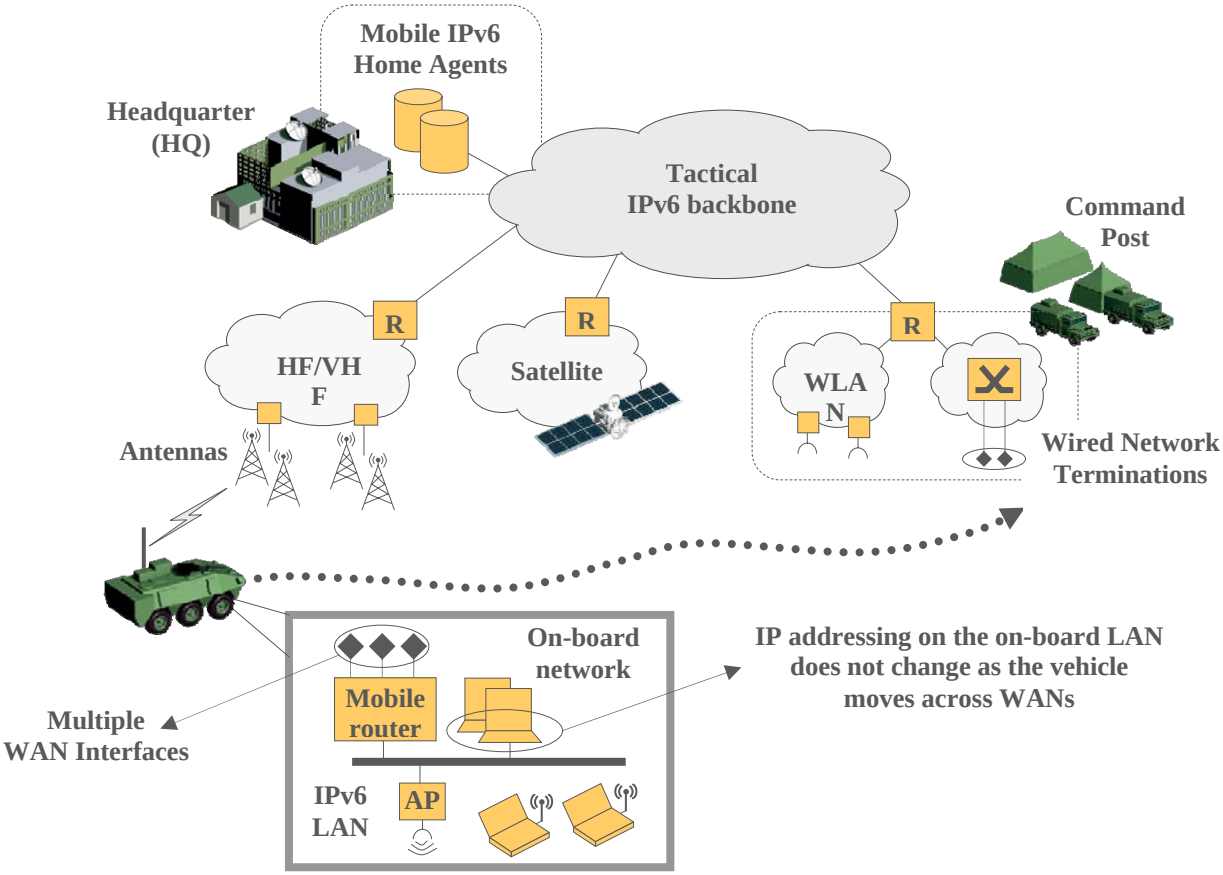

Figure A. 4 Basic NEMO Scenario

In a typical operational scenario, the military vehicle can exploit HF/VHF or satellite while in the battlefield, and can relay on high-speed links, like WLAN or Ethernet, when parked in a command post. NEMO technology allows all of these movements across access WANs to take place transparently. All active communications survive movements and there is no need to re-configure the PCs or other appliances located on the on-board LAN, which can be made constantly reachable at their long-lived IPv6 addresses.

Moreover, even though the scenario in ***Figure A. 4***[15] refers to vehicles moving on the ground, the same concepts can be applied to ships or other naval units. For example, using NEMO, it would be possible for a ship docked at a port to switch from satellite to cable connections without the need of any manual intervention on the on-board equipment.

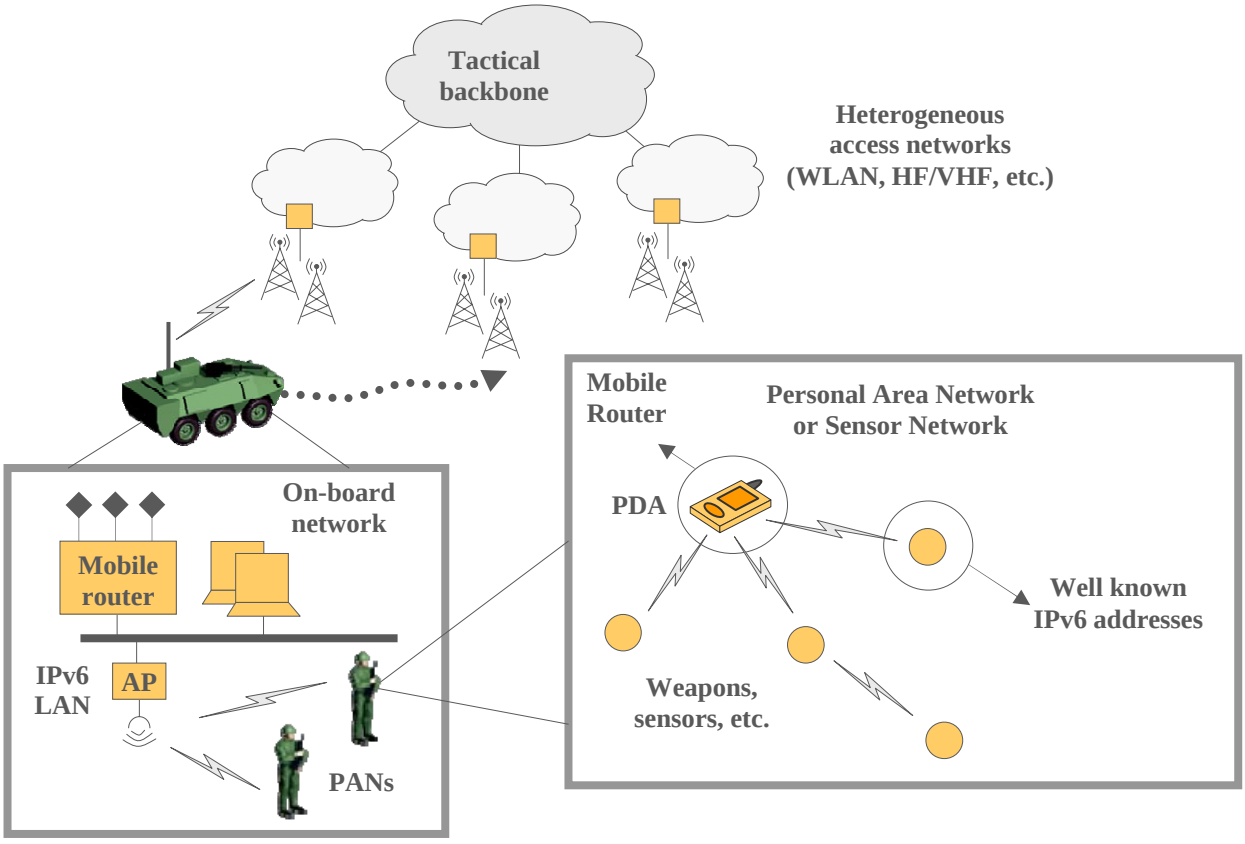

Figure A. 5 Nested NEMO Scenario

Figure A. 5 [15] shows an example of nested NEMO scenario. It is assumed that the military vehicle hosts one or more soldiers, each equipped with a PDA (or another personal equipment) providing connectivity to a set of wearable tools (weapons, healthcare sensors, etc.). The PDA and the other tools form a Personal Area Network (PAN), which can be managed as a "personal moving network", with the PDA running the NEMO protocol (i.e. the PDA is the mobile router). This way, each PAN is permanently reachable independently of the actual location of the soldier.

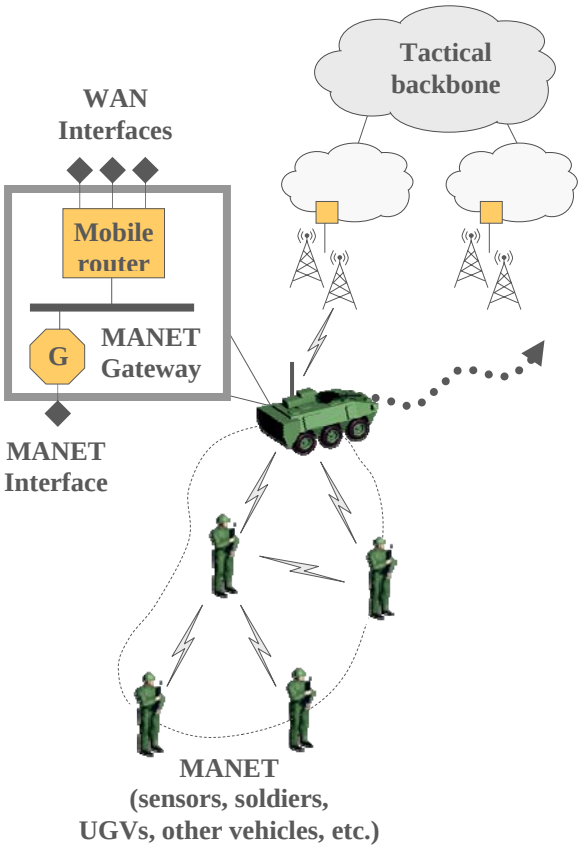

Figure A. 6 Combined Usage of NEMO and MANET

Figure A. 6 [15] shows an example of how NEMO and MANET can be used together. The simplest option is to have a moving network providing WAN connectivity to a MANET. In this case, the WAN interface of the MANET gateway is connected to the on-board LAN and the MANET gateway can be either implemented as a standalone machine or co-located with the mobile router. As a result, the MANET can benefit from mobile connectivity to the tactical IPv6 backbone.

A.5.2 NEMO Applicability to Military Tactical Scenario

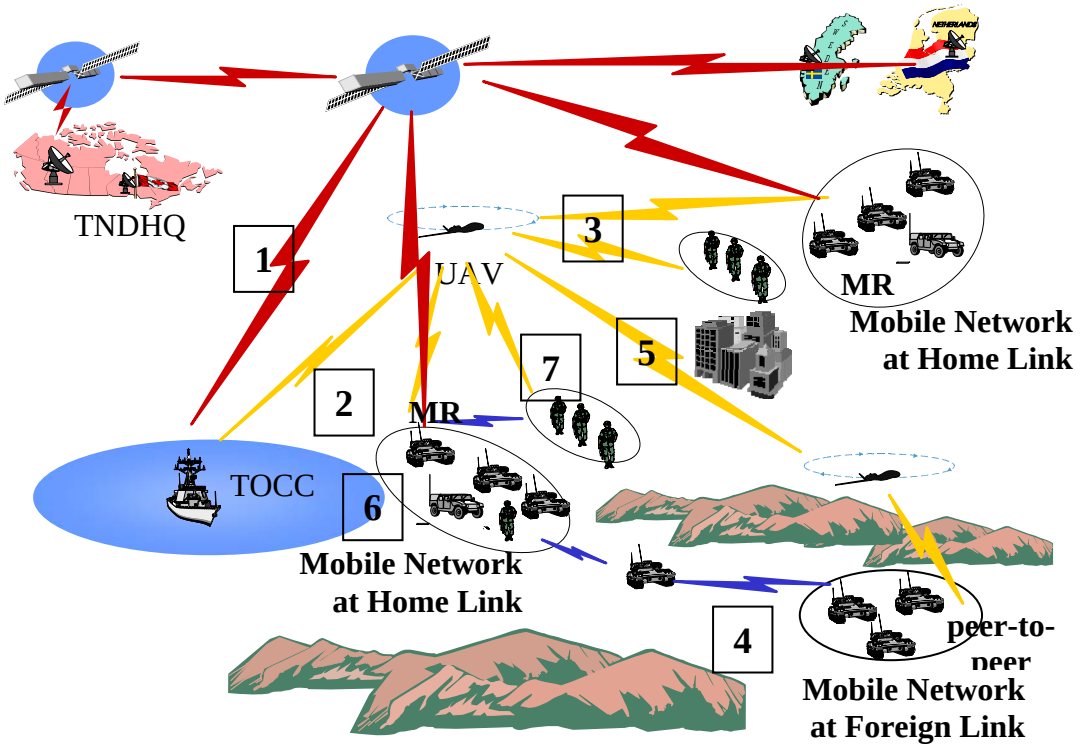

Figure A. 7 NEMO Applicability

Given the scenario described in Section 1 as shown in ***Figure A. 8***, some tanks or APVs or ground troops may have dedicated satellite links for connectivity with their national defense headquarters. If NEMO technology is supported in the network and the tanks or APVs or ground troops serve as MRs for other participating forces, then these participants can also have connectivity with their home networks as well as with outside networks. The MRs with satellite links reside in their home network from a routing perspective. An MN or a mobile network from different networks can attach to those MRs. An MR equipped with a satellite link will tunnel outgoing packets sent from an attached MN or an attached mobile network and detunnel incoming packets for the attached MN or nodes in the attached mobile network. When a group of tanks, APVs, or soldiers move around the tactical area, as long as their MRs connect to other MRs with satellite links, they will be able to communicate with networks outside this area even when their MRs do not have satellite links. This is the NEMO scenario,

which is exemplified in ***Figure A. 4*** [15]. The connectivity to the MR with satellite links can be achieved in one hop in the case of the WLAN, or in multiple hops away from the MR in the MANET case. For example, a group of tanks consist of a MANET. One of the tanks with a satellite link acts as an MR, while another group of soldiers with a tank moves into the MANET area. The tank is an MR for this group of soldiers. The MR without a satellite link will attach to the MR with a satellite link through the MANET and acquires a COA from the MR with a satellite link. The example in ***Figure A. 6*** [15] explains how NEMO and MANET can be used together.

List of Abbreviations

DRDC	Defence R&D Canada
CRC	Communications Research Centre
MANET	Mobile Ad Hoc Network
OLSR	Optimized Link State Routing Protocol
H-OLSR	Hierarchical Optimized Link State Routing Protocol
LANMAR	Landmark Ad Hoc Routing Protocol
H-LANMAR	Hierarchical Landmark Ad Hoc Routing Protocol
FSR	Fisheye State Routing
MPR	Multiple Point Relay
HELLO	Hello message
TC	Topology Control
HTC	Hierarchical Topology Control
CIA	Cluster ID Announcement
LSR	Link State Routing
LUM	LANMAR Update Message
DFDV	Drifter For Distance Vector
ISR	Intelligence Surveillance Reconnaissance
TOCC	Tactical Operational Command Centre
TNDHQ	TransNational Defence HeadQuarters
UAV	Unmanned Aerial Vehicles
APR	Armoured Personnel Vehicles

FLOT	Front Line of Own Troops
WAN	Wide Area Network
HQ	Headquarters
AODV	Ad-Hoc On-Demand Distance Vector Routing Protocol
ZRP	Zone Routing Protocol
DSR	Dynamic Source Routing
MAC	Medium-access control
UCLA	University of California Los Angeles
RPGM	Reference Point Group Mobility
NEMO	NEtwork MObility
MN	Mobile Node
HA	Home Agent
COA	Care-Of Address
CN	Correspondent Node
MR	Mobile Router
PAN	Personal Area Network
LAN	Local Area Network
WLAN	Wireless Local Area Network
PDA	Personal Digital Assistant

DOCUMENT CONTROL DATA

(Security classification of title, body of abstract and indexing annotation must be entered when the overall document is classified)

1. ORIGINATOR (the name and address of the organization preparing the document. Organizations for whom the document was prepared, e.g. Establishment sponsoring a contractor's report, or tasking agency, are entered in section 8.)

Communication Research Center
3701 Carling Av, Ottawa, Ontario
K2H 8S2

2. SECURITY CLASSIFICATION (overall security classification of the document, including special warning terms if applicable)

UNCLASSIFIED

3. TITLE (the complete document title as indicated on the title page. Its classification should be indicated by the appropriate abbreviation (S,C or U) in parentheses after the title.)

Comparison of Two Hierarchical Routing Protocols for Heterogeneous MANET (U)

4. AUTHORS (Last name, first name, middle initial)

Wang, Maoyu , Ge, Ying, Lamont, Louise

5. DATE OF PUBLICATION (month and year of publication of document)	6a. NO. OF PAGES (total containing information. Include Annexes, Appendices, etc.)	6b. NO. OF REFS (total cited in document)
October 2007	74	17

7. DESCRIPTIVE NOTES (the category of the document, e.g. technical report, technical note or memorandum. If appropriate, enter the type of report, e.g. interim, progress, summary, annual or final. Give the inclusive dates when a specific reporting period is covered.)

Technical Memorandum

8. SPONSORING ACTIVITY (the name of the department project office or laboratory sponsoring the research and development. Include the address.)

Defence R&D Canada - Ottawa
3701 Carling Avenue
Ottawa, Ontario, K1A 0Z4

9a. PROJECT OR GRANT NO. (if appropriate, the applicable research and development project or grant number under which the document was written. Please specify whether project or grant)	9b. CONTRACT NO. (if appropriate, the applicable number under which the document was written)
15BR	

10a. ORIGINATOR'S DOCUMENT NUMBER (the official document number by which the document is identified by the originating activity. This number must be unique to this document.)	10b. OTHER DOCUMENT NOS. (Any other numbers which may be assigned this document either by the originator or by the sponsor)
DRDC Ottawa TM 2007-201	

11. DOCUMENT AVAILABILITY (any limitations on further dissemination of the document, other than those imposed by security classification)

(x) Unlimited distribution
( ) Distribution limited to defence departments and defence contractors; further distribution only as approved
( ) Distribution limited to defence departments and Canadian defence contractors; further distribution only as approved
( ) Distribution limited to government departments and agencies; further distribution only as approved
( ) Distribution limited to defence departments; further distribution only as approved
( ) Other (please specify):

12. DOCUMENT ANNOUNCEMENT (any limitation to the bibliographic announcement of this document. This will normally correspond to the Document Availability (11). However, where further distribution (beyond the audience specified in 11) is possible, a wider announcement audience may be selected.)

Unlimited

13. ABSTRACT (a brief and factual summary of the document. It may also appear elsewhere in the body of the document itself. It is highly desirable that the abstract of classified documents be unclassified. Each paragraph of the abstract shall begin with an indication of the security classification of the information in the paragraph (unless the document itself is unclassified) represented as (S), (C), or (U). It is not necessary to include here abstracts in both official languages unless the text is bilingual).

In this report, a study on hierarchical routing protocols for heterogeneous mobile Ad Hoc wireless networks is presented. The main thrust of the investigation is to identify a potential hierarchical routing scheme that is best suited for a heterogeneous tactical Mobile Ad Hoc Network (MANET). Such networks consist of mobile nodes that are characterized by different communications capabilities, such as multiple radio interfaces. The report highlights the benefits and issues of the different routing protocols, namely the H-OLSR and H-LANMAR, as it pertains to a military tactical scenario. We first discuss the context for the use of a hierarchical routing strategy by describing a typical military scenario where a number of platforms are used each supporting link types of varying capabilities. We then discuss the rational for selecting a proactive hierarchical routing scheme for typical tactical MANETs. We discuss in detail the routing algorithms of the two protocols under investigation. Finally we conduct an experimental comparison study between the two routing protocols.
Our experiments reveal that H-OLSR outperforms H-LANMAR for most of the group mobility scenarios that can potentially be used in the operation of a tactical MANET.

14. KEYWORDS, DESCRIPTORS or IDENTIFIERS (technically meaningful terms or short phrases that characterize a document and could be helpful in cataloguing the document. They should be selected so that no security classification is required. Identifiers such as equipment model designation, trade name, military project code name, geographic location may also be included. If possible keywords should be selected from a published thesaurus. e.g. Thesaurus of Engineering and Scientific Terms (TEST) and that thesaurus-identified. If it is not possible to select indexing terms which are Unclassified, the classification of each should be indicated as with the title.)

Heterogeneous MANET routing protocol, H-OLSR, H-LANMAR, Heterogeneous tactical MANET Network

Defence R&D Canada

Canada's leader in Defence
and National Security
Science and Technology

R & D pour la défense Canada

Chef de file au Canada en matière
de science et de technologie pour
la défense et la sécurité nationale

www.drdc-rddc.gc.ca